VICON

User Guide

XX247-00-05

V-CELL High-Security Corner-Mount Cameras

Vicon Industries Inc.

Tel: 631-952-2288 Fax: 631-951-2288 Toll Free: 800-645-9116

24-Hour Technical Support: 800-34-VICON (800-348-4266) UK: 44/(0) 1489-566300

Vicon Industries Inc. does not warrant that the functions contained in this equipment will meet your requirements or that the operation will be entirely error free or perform precisely as described in the documentation. This system has not been designed to be used in life-critical situations and must not be used for this purpose.

www.vicon-security.com

Document Number: 8009-8247-00-05

Issued: 214

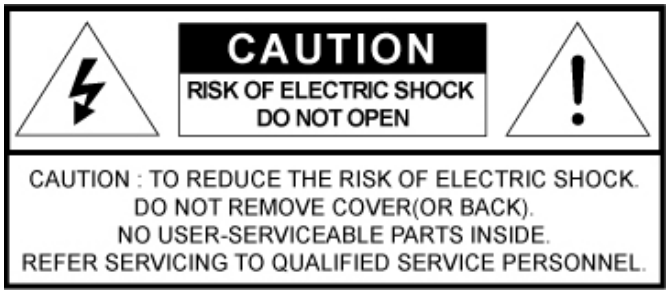
Product specifications subject to change without notice.

Copyright © 2014 Vicon Industries Inc. All rights reserved.

WARNING

TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. DO NOT INSERT ANY METALLIC OBJECT THROUGH THE VENTILATION GRILLS OR OTHER OPENNINGS ON THE EQUIPMENT.

CAUTION


CAUTION
RISK OF ELECTRIC SHOCK
DO NOT OPEN
CAUTION : TO REDUCE THE RISK OF ELECTRIC SHOCK.
DO NOT REMOVE COVER(OR BACK).
NO USER-SERVICEABLE PARTS INSIDE.
REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.

EXPLANATION OF GRAPHICAL SYMBOLS

The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of uninsulated "dangerous voltage" within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock.

The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

PRECAUTIONS

Safety ---------- Installation ----------

Should any liquid or solid object fall into the cabinet, unplug the unit and have it checked by the qualified personnel before operating it any further.

Unplug the unit from the wall outlet if it is not going to be used for several days or more. To disconnect the cord, pull it out by the plug. Never pull the cord itself.

Allow adequate air circulation to prevent internal heat build-up. Do not place the unit on surfaces (rugs, blankets, etc.) or near materials (curtains, draperies) that may block the ventilation holes.

Height and vertical linearity controls located at the rear panel are for special adjustments by qualified personnel only.

Do not install the unit in an extremely hot or humid place or in a place subject to excessive dust, mechanical vibration.

The unit is not designed to be waterproof.
Exposure to rain or water may damage the unit.

Cleaning ----------

Clean the unit with a slightly damp soft cloth.
Use a mild household detergent. Never use strong solvents such as thinner or benzene as they might damage the finish of the unit.

Retain the original carton and packing materials for safe transport of this unit in the future.

FCC COMPLIANCE STATEMENT

INFORMATION TO THE USER: THIS EQUIPMENT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE LIMITS FOR A CLASS A DIGITAL DEVICE, PURSUANT TO PART 15 OF THE FCC RULES. THESE LIMITS ARE DESIGNED TO PROVIDE REASONABLE PROTECTION AGAINST HARMFUL INTERFERENCE WHEN THE EQUIPMENT IS OPERATED IN A COMMERCIAL ENVIRONMENT. THIS EQUIPMENT GENERATES, USES, AND CAN RADIATE RADIO FREQUENCY ENERGY AND IF NOT INSTALLED AND USED IN ACCORDANCE WITH THE INSTRUCTION MANUAL, MAY CAUSE HARMFUL INTERFERENCE TO RADIO COMMUNICATIONS.

CAUTION: CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

THIS CLASS A DIGITAL APPARATUS COMPLIES WITH CANADIAN ICES-003.

CET APPAREIL NUMÉRIQUE DE LA CLASSE A EST CONFORME À LA NORME NMB-003 DU CANADA.

CE COMPLIANCE STATEMENT

WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

IMPORTANT SAFETY INSTRUCTIONS

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.

13. Unplug this apparatus during lightning storms or when unused for long periods of time.
14. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
15. ***CAUTION – THESE SERVICING INSTRUCTIONS ARE FOR USE BY QUALIFIED SERVICE PERSONNEL ONLY. TO REDUCE THE RISK OF ELECTRIC SHOCK DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE OPERATING INSTRUCTIONS UNLESS YOU ARE QUALIFIED TO DO SO.***
16. ***Use satisfy clause 2.5 of IEC60950-1/UL60950-1 or Certified/Listed Class 2 power source only.***
17. ITE is to be connected only to PoE networks without routing to the outside plant.

Contents

1. Description ----------6

1.1 Components-- ---------- 6

1.2 Key Features - ---------- 7

2. Installation ---------- 8

2.1 Parts and Description ----------8

2.2 Quick Installation ----------9

2.3 Unpacking and Inspection ----------13

2.4 Physical Installation ----------13

2.5 Network Connection and IP Assignment ---------- 21

3. Operation ---------- 22

3.1 Access from a browser ---------- 22

3.2 Access from the internet ---------- 23

3.3 Setting the admin password over a secure connection ---------- 23

3.4 Live View Page---------- 24

3.5 Network Camera Setup---------- 27

3.5.1 Basic Configuration---------- 27

1) Users---------- 27

2) Network ---------- 28

3) Video & Image ---------- 29

4) Audio---------- 31

5) Date & Time ---------- 33

3.5.2 Video & Image---------- 34

3.5.3 Audio ---------- 37

3.5.4 Event ---------- 38

1) Event-In ---------- 38

2) Event-Out ---------- 43

3) Event Map---------- 49

3.5.5 System ---------- 50

1) Information ---------- 50

2) Security---------- 51

3) Date & Time ---------- 54

4) Network ---------- 55

5) Language---------- 64

6) Maintenance ---------- 65

7) Support ---------- 66

3.6 Playback ---------- 67

3.7 Help---- ---------- 69

3.8 Resetting to the factory default settings---------- 70

4. Appendix ---------- 71

4.1 Troubleshooting---------- 71

4.2 Alarm Connection ---------- 72

4.3 Preventive Maintenance ---------- 72

4.3 Product Specification---------- 73

1. Description

The information in this manual provides quick installation and setup procedures for the V-CELL series of High-Security Corner-Mounted Cameras. These units should only be installed by a qualified technician using approved materials in conformance with federal, state, and local codes. Read these instructions thoroughly before beginning an installation. Refer to the complete manual for detailed information. Always refer to Vicon's website to assure you have the most up-to-date manual, http://www.vicon-security.com.

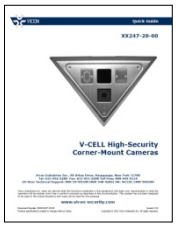
The Roughneck® V-CELL high-security camera is an integrated housing, camera, lens and IR illuminators system specifically designed for use in custodial suites and prison cells. It is available in an analog version and IP version that is fully compatible with all ViconNet® systems; its ONVIF certification provides an open-platform for integration into other video management systems.

The housing is designed to fit into a corner; once installed, the base plate should be permanently sealed to the wall so that the housing is ligature proof. The housing consists of a two part stainless steel assembly, a fixed base plate and a removable front plate, that allows ease of installation and servicing. The front plate is secured with security screws and has two polycarbonate windows to protect the camera and IR illuminators. The alarm input and alarm output can be used to connect various third party devices, such as door sensors and alarm bells.

1.1 Components

The system comes with the following components:

Camera unit



Quick Installation Guide

Installation CD

Accessory Kit

Note: Check your package to make sure that you received the complete system, including all components shown above.

1.2 V-CELL-IP Key Features

- **Brilliant video quality**
  The Network Camera offers the highly efficient H.264 video compression, which drastically reduces bandwidth and storage requirements without compromising image quality. Motion JPEG is also supported for increased flexibility.

- **Dual or Triple streams**
  The Network Camera can deliver dual or triple video streams simultaneously at full frame rate in all resolutions up to 4CIF(704x480 or 704x576) using Motion JPEG and H.264 (or MPEG-4). This means that several video streams can be configured with different compression formats, resolutions and frame rates for different needs.

- **Image setting adjustment**
  The Network Camera also enables users to adjust image settings such as contrast, brightness and saturation to improve images before encoding takes place.

- **Intelligent video capabilities**
  The Network Camera includes intelligent capabilities such as enhanced video motion detection. The camera's external inputs and outputs can be connected to devices such as sensors and relays, enabling the system to react to alarms and activate lights or open/close doors.

- **Micro-SD Recording support**
  The Network Camera also supports a micro-SD memory slot for local recording with removable storage.

- **Improved Security**
  The Network Camera logs all user access, and lists currently connected users. Also, its full frame rate video can be provided over HTTPS.

- **Power over Ethernet**
  Support for Power over Ethernet (IEEE802.3af) enables the unit, as well as the camera module that is connected to it, to receive power through the same cable as for data transmission. This makes for easy installation since no power outlet is needed.

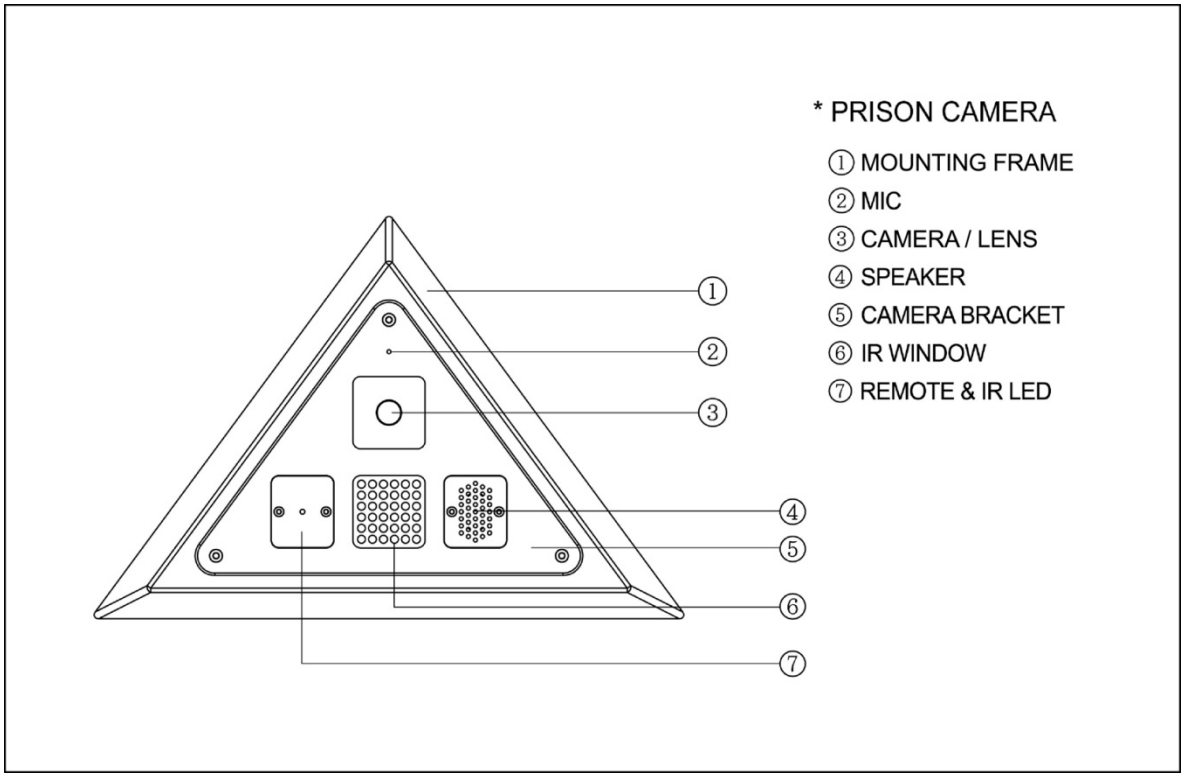
- **ONVIF**
  This is a global interface standard that makes it easier for end users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperability between different vendor products, increased flexibility, reduced cost, and future-proof systems.

- **IR illumination**
  36 IR LED illuminators (940nm with low visibility) light up to 66 ft (20m); intensity; adjustable.

- **Audio In/Out**
  1 Mic/1 Speaker (G.711)

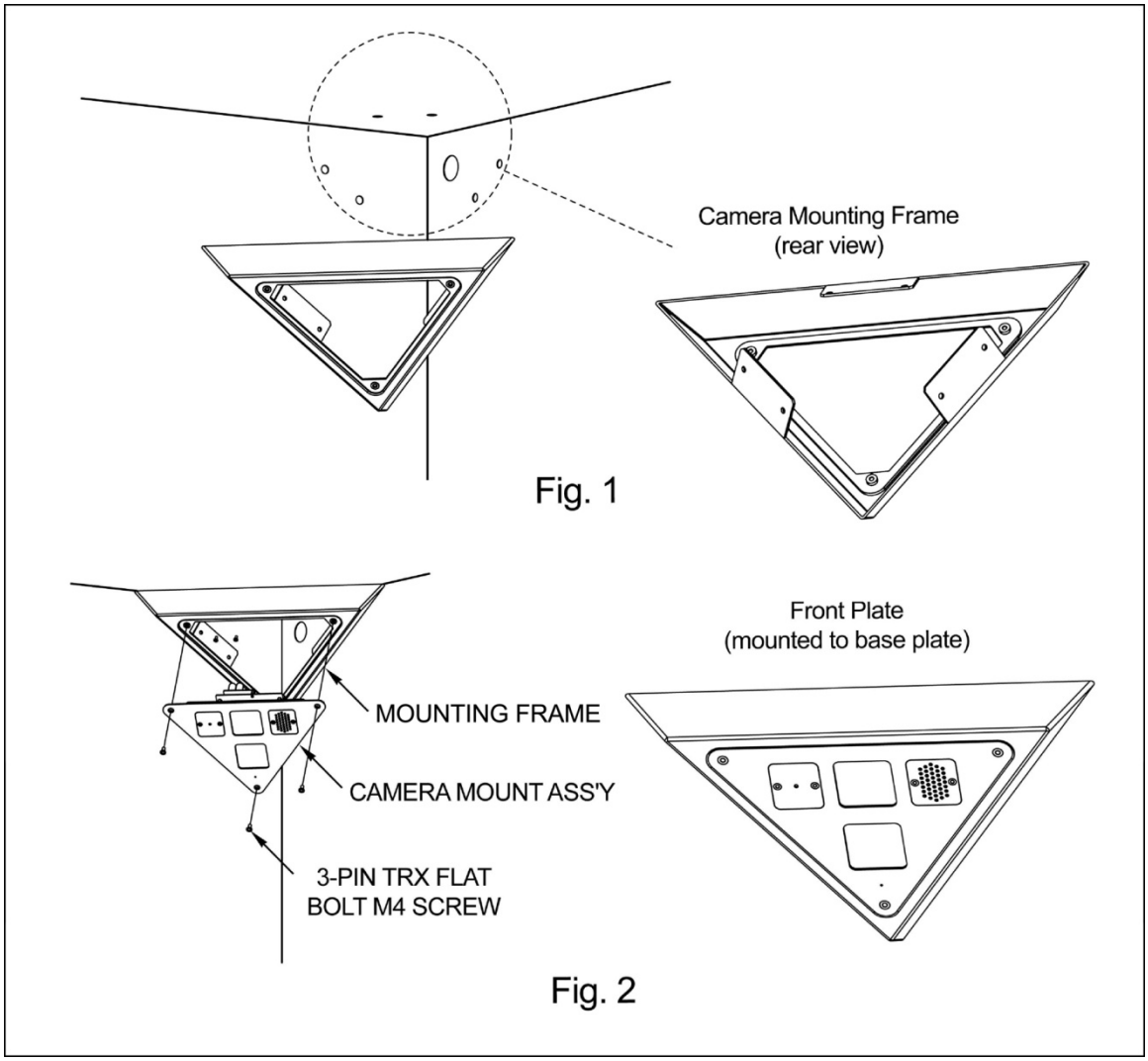
2. Installation

2.1 Parts and Description



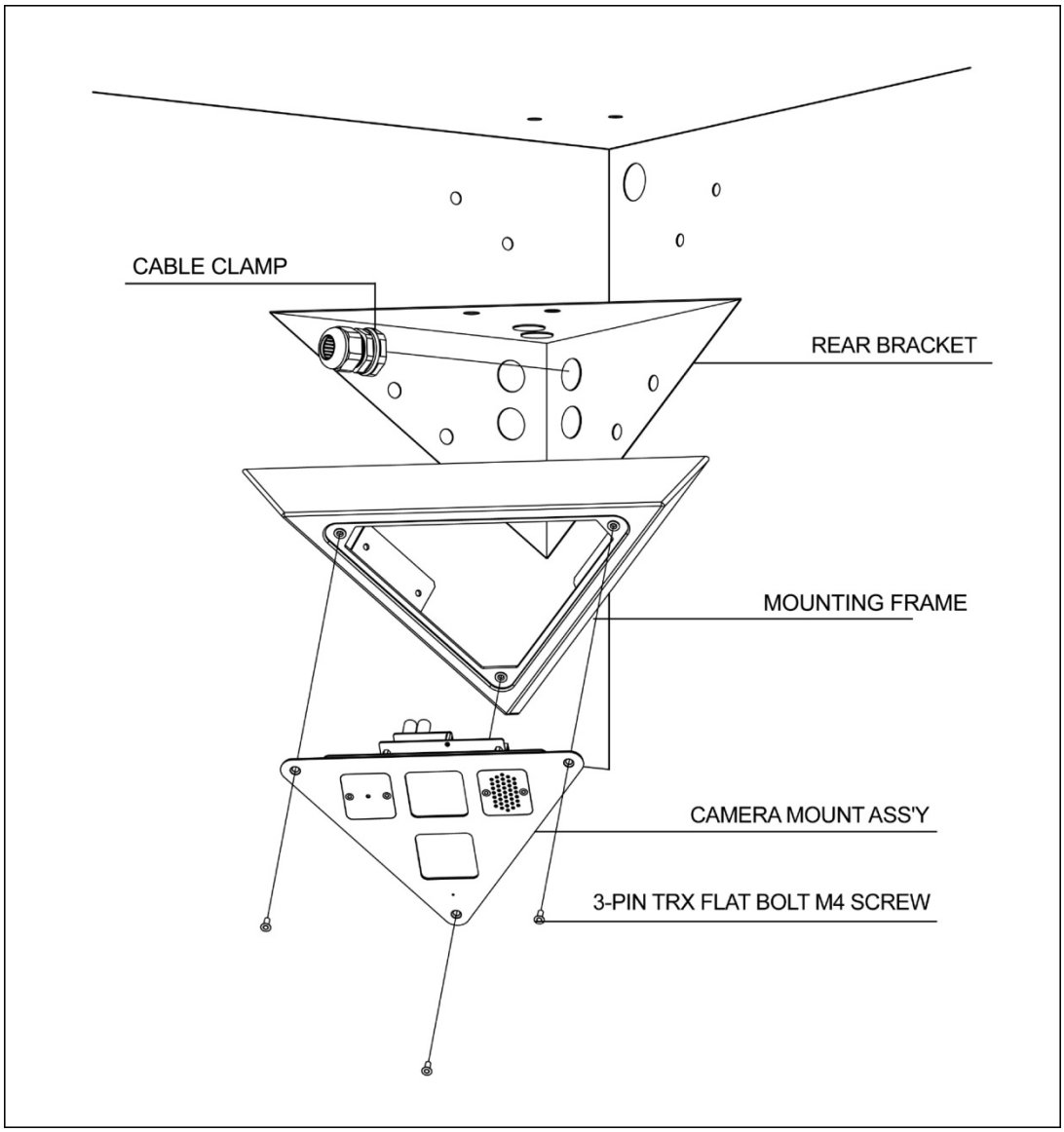
2.2 Quick Installation

Below is an overview for installing the V-CELL camera. When using rear cover, refer to the diagram that follows. Detailed instructions follow.



1. Use camera mounting frame as template to mark mounting holes on mounting surface. (Fig.1)
2. Drill holes for mounting base and a minimum 3/4 in. hole for routing wines. (Fig.1)
3. Mount camera mounting frame using appropriate hardware for mounting surface. (Fig.2)
4. Route wires through hole in wall and out through base plate. (Fig.2).
5. Terminate wires to camera board.
6. Mount front plate to base plate. (Fig.2)

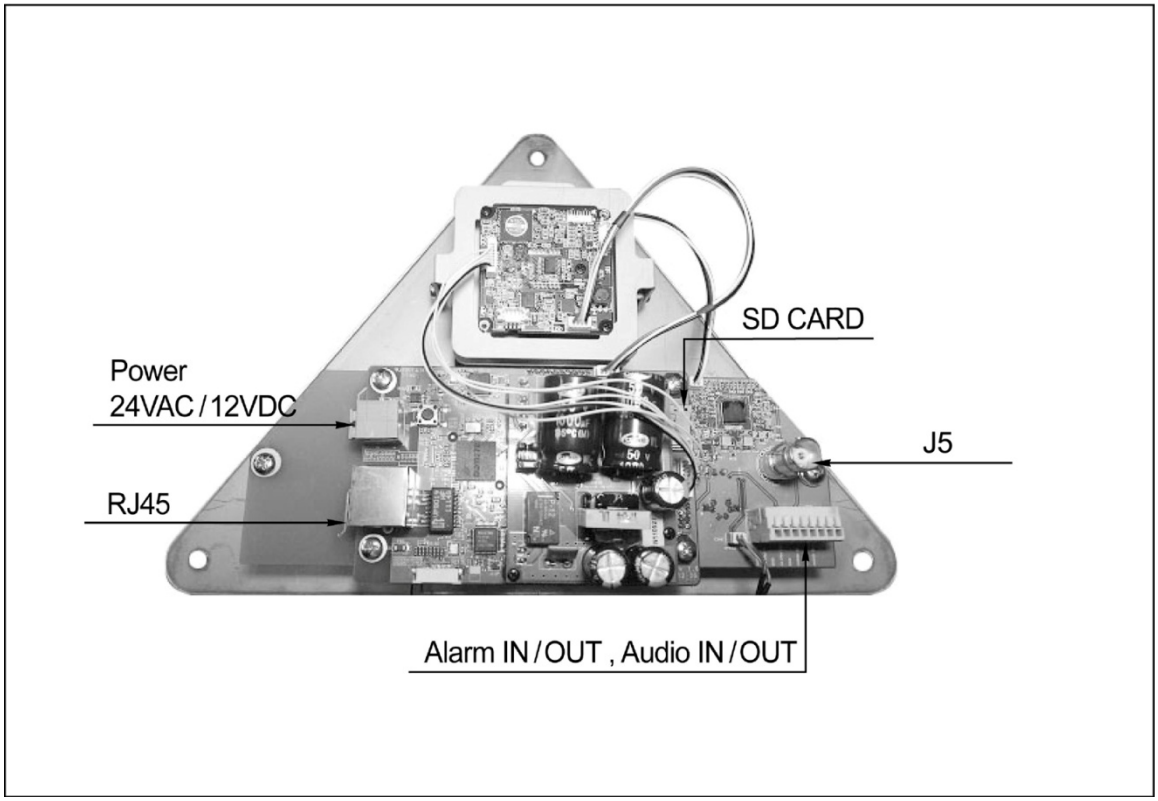
When using rear cover, follow diagram below.



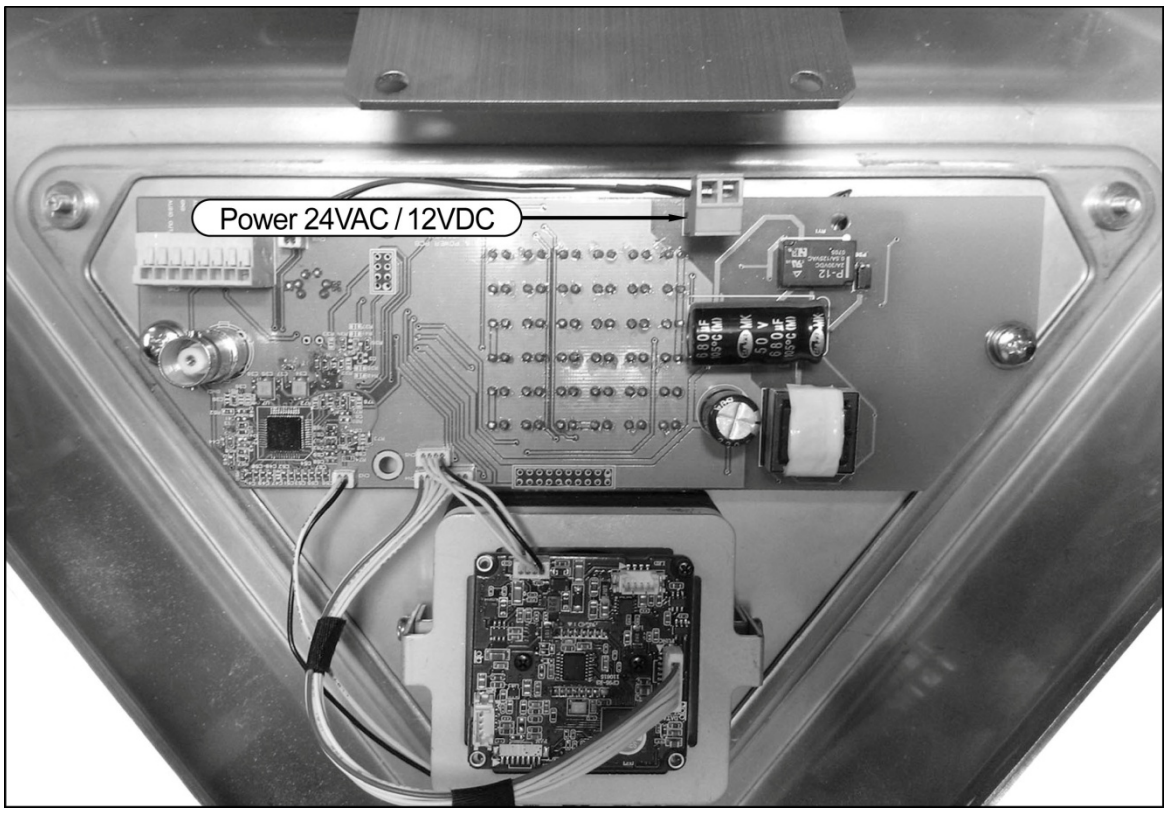
1. Use rear cover as template to mark mounting and cable access holes.
2. Drill mounting and cable access holes in mounting surface.
3. Insert cable clamp into access hole, route cables through clamp and mount cover using appropriate hardware.
4. Use camera mounting frame to mark its mounting holes, drill holes and mount using appropriate hardware.
5. Terminate wires to camera board. Feed the excess wire back through cable clamp and tighten clamp.
6. Mount front plate to camera mounting frame.

Installation of the rear cover is required for UL/Canadian UL compliance.

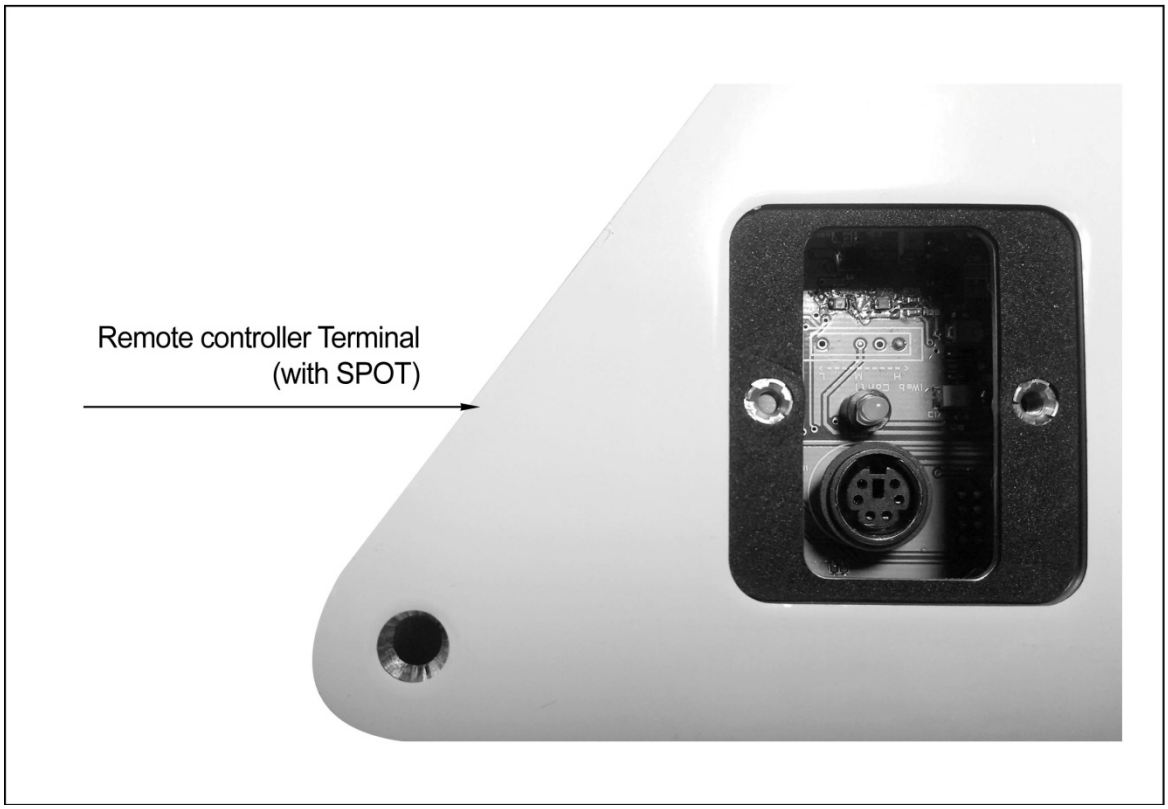
- IP Camera



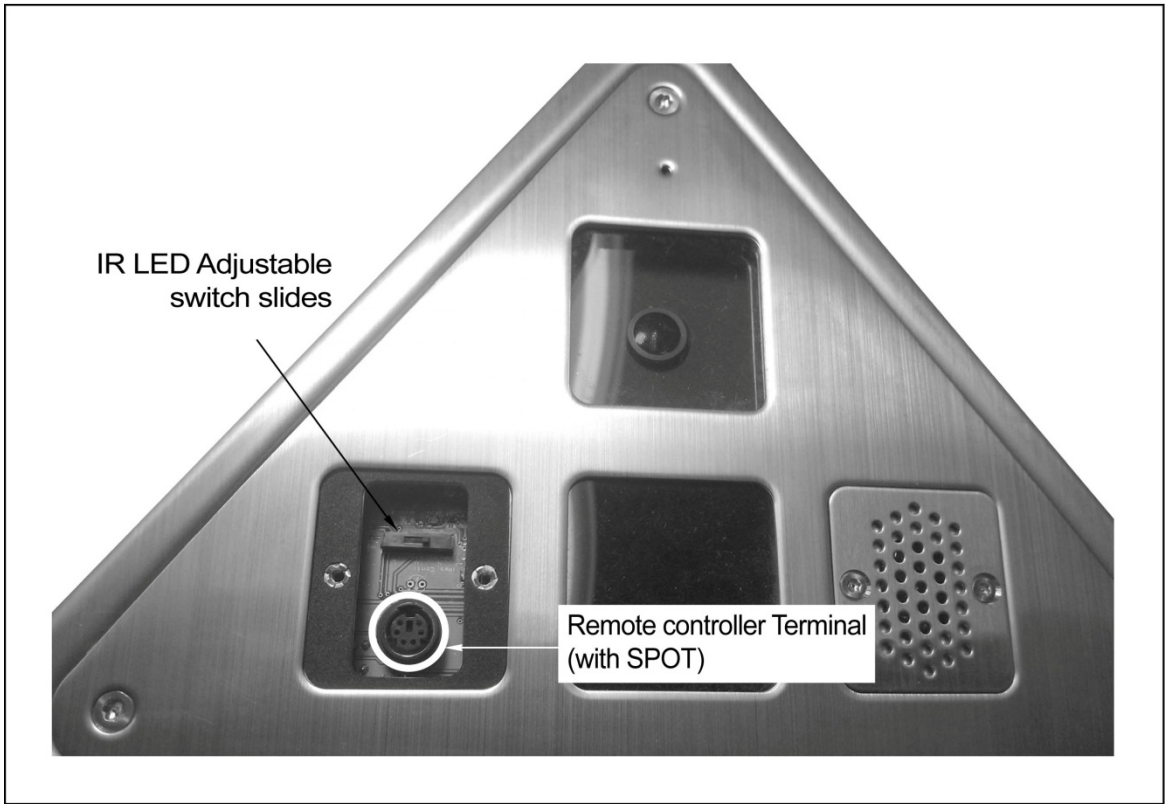
- Analog Camera



- IP Camera



- Analog Camera



2.3 Unpacking and Inspection

All Vicon equipment is inspected and tested before leaving the factory. It is the carrier's responsibility to deliver the equipment in the same condition in which it left the factory.

Inspection for Visible Damage
Immediately inspect the cartons upon delivery. On all copies of the carrier's freight bill, make a note of any visible damage.

Make sure the carrier's agent (the person making the delivery) signs the note on all copies of the bill. If the agent does not have claim forms, contact the carrier's office.

Inspection for Concealed Damage
As soon as possible after delivery, unpack the unit and inspect it for concealed damage. Do not discard the carton or packing materials. If the unit is damaged, contact the carrier immediately and request forms for filing a damage claim. Make arrangements for a representative of the carrier to inspect the damaged equipment.
If the equipment must be returned for repair, follow the Shipping Instructions at the end of this document.

2.4 Physical Installation

The V-CELL is designed to fit into a corner where two walls and a ceiling meet. It is fastened to both walls and the ceiling. Refer to Figure 1. Cable access is provided by removing the front plate. The camera has an adjustable mount that may be tilted slightly to give a precise angle of view. A 2.5 mm wide angle lens enables the camera to view the cell with no "blind spots;" 36 IR LED illuminators are provided to light up to 66 ft (20 m).

The wall/ceiling material must provide suitable strength to support the weight of the unit (3.5 lb/1.6 kg). Be sure the area around the selected location is clear of obstacles (such as steel beams, headers, pipes, electrical wiring, etc.) that would interfere with mounting. All cables must be routed to the installation location. Before beginning installation, read the Cable Recommendations at the end of this manual and verify that the accessory pack contains the items listed in below table.

Item	Quantity	Function
No. 20 Torx Bit	1	Use to remove and install tamperproof screws from front plate
No. 20 Torx Bit	1	Use to remove and install tamperproof screws from front plate access cover plate
2-Pin Terminal Block	1	Use to make power cable connections
Back Cover	1	Fire barrier; ***required for UL/cUL compliance***
Quick Guide/Documentation CD/ ViconNet CD (IP versions)	1	Installation and operation instructions; ViconNet setup CD

Mounting the Housing

The housing consists of two main assemblies, the camera mounting frame and the removable front plate, where the camera and all electronics are mounted. The front plate is secured to the base plate with Resistorx tamperproof screws. A special bit is supplied in the accessory pack for removing and replacing these screws. When the installation is complete, retain the Torx bit in case access to the

interior of the housing is required later. Additionally, a rear cover is supplied for those installations requiring Canadian UL compliance or extra protection from fire.

Installation without the rear cover:

1. Remove the front plate using the no. 20 Torx bit provided; retain the screws in a safe place. Using the camera mounting frame as a template, mark the locations of the mounting holes on the three mounting tabs (2 holes per tab). Open a hole in the wall or ceiling to accommodate routing the cables to the camera.
2. Route all necessary cables to the location if not already done so.
3. Drill suitable holes for the hardware selected appropriate for the wall/ceiling material. The use of No. 8 (or 4 mm metric) mounting hardware is recommended. Use hollow-wall anchors or, if the housing is being mounted on a sheet metal surface, use rivet nuts.
4. Secure the camera mounting frame to the wall/ceiling with fasteners appropriate for the mounting surface. Route the cables through the access hole in the wall or ceiling.
5. When the camera mounting frame is secured to the surface, apply an epoxy security sealant around the perimeter of the base plate where it meets the ceiling/wall. [Vicon recommends DynaPoxy™ EP1200 (US) or Arbokol 1025 (UK) or equivalent for this purpose.]

Installation with the rear cover:

Note: The installation corner must be sharp and clean; if necessary, clean any excess material from the installation location.

1. Remove the front plate using the no. 20 Torx bit provided; retain the screws in a safe place.
2. Select the cable access hole in the rear cover to be used (6 provided) and knockout the hole. Place the rear cover in the corner; using it as a template, mark the locations of the three (3) mounting holes and the cable access hole. Remove it from the corner.
3. Drill suitable mounting holes and open the hole to accommodate routing the cables to the camera in the wall/ceiling. Be sure the cable access hole is large enough to accommodate the cable clamp.
4. Route all necessary cables to the location if not already done so. Fasten the cable clamp (provided) into the cable access knockout hole so that the clamp is on the inside of the rear cover. Route cables through the access hole and through the rear cover; be sure to allow enough cable length to make connections to the camera board. Mount the rear cover to the wall/ceiling through the 3 holes provided; use hardware appropriate for the mounting surface.
5. Using the camera mounting frame as a template, insert it into the rear cover and mark the mounting holes on the 3 tabs (2 holes per tab) that align with the holes in the rear cover; drill suitable mounting holes. Attach the camera mounting frame onto the wall/ceiling and secure it using appropriate hardware for the mounting surface. The use of No. 8 (or 4 mm metric) mounting hardware is recommended. Use hollow wall anchors or, if the housing is being mounted on a sheet metal surface, use rivet nuts.
6. Make cable connections to the camera board. See instructions below. Adjust the cable length as necessary and secure the cable clamp.

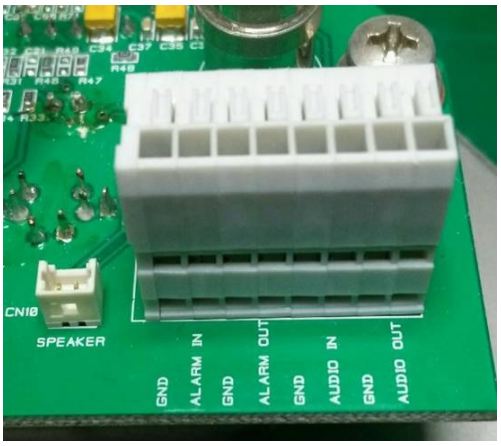
Caution: *Installation of the rear cover is required for UL/Canadian UL compliance.*

7. When the camera mounting frame assembly is secured to the surface, apply an epoxy security sealant around the perimeter of the base plate assembly where it meets the ceiling/wall. [Vicon recommends DynaPoxy™ EP1200 (US) or Arbokol 1025 (UK) or equivalent for this purpose.]

Cable Connections

All cabling is done to the boards located on the back of the front plate.

Note: *Vicon systems and components, like most electronic equipment, require a clean, stable power source. Voltage irregularities such as surges, drops, and interruptions can affect the operation of your equipment and, in severe cases, damage certain components.*



8-pin terminal block on board.
Pinouts are as follows (printed on the board):
Pin1 : AUDIO OUT
Pin 2 : GND
Pin.3 : AUDIO IN
Pin4 : GND
Pin.5 : ALARM Out
Pin 6 : GND
Pin 7 : ALARM IN(IP Only)
Pin 8 : GND

Analog Cable Connections

1. Connect the power cable to the 2-postion terminal block. The camera accepts 24 VAC (or 12 VDC) and polarity is not relevant.
2. Connect the coaxial cable for video output to the BNC connector.
3. To adjust the intensity of the LED illuminators, use switch slides. The factory setting is for maximum intensity.
4. Connect the device to the AO (Alarm Out) and G (Ground) terminal block connectors. Alarm Out can activate external devices such as buzzers or lights. There is no AI (Alarm In). Connect the Audio In and Out as needed. Pinouts for the terminal block are printed on the board. Refer to figure above.

IP Cable Connections

1. Use the RJ-45 connector if powering the camera using PoE. If using 24 VAC (or 12 VDC), connect the power cable to the 2-postion terminal block. Connect the positive (+) pole to the '+' position and the negative (-) pole to the '-' position. Use certified/Listed Class 2 power source only.
2. Video and data are transmitted via the RJ-45 connector. Generally a cross-over cable is used for direct connection to PC, while a direct cable is used for connection to a hub.
3. To adjust the intensity of the LED illuminators, use web control. The factory setting is for maximum intensity.
4. Alarm connections: **AI (Alarm In):** External devices can signal the network camera to react on events. Mechanical or electrical switches can be wired to the AI (Alarm In) and G (Ground) terminal block connectors. **G (Ground):** Connect the ground side of the alarm input and/or alarm output to the G (Ground) connector. **Alarm Out:** The network camera can activate external devices such as buzzers or lights. Connect the device to the AO (Alarm Out) and G (Ground) terminal block connectors. Connect the Audio In and Out as needed. Pinouts for the terminal block are printed on the board. Refer to figure above.
5. **Connecting Video Output:** Video Output is provided for an easy zoom and focus control when adjusting lens. Connect your Video cable unit to J5 on the board.

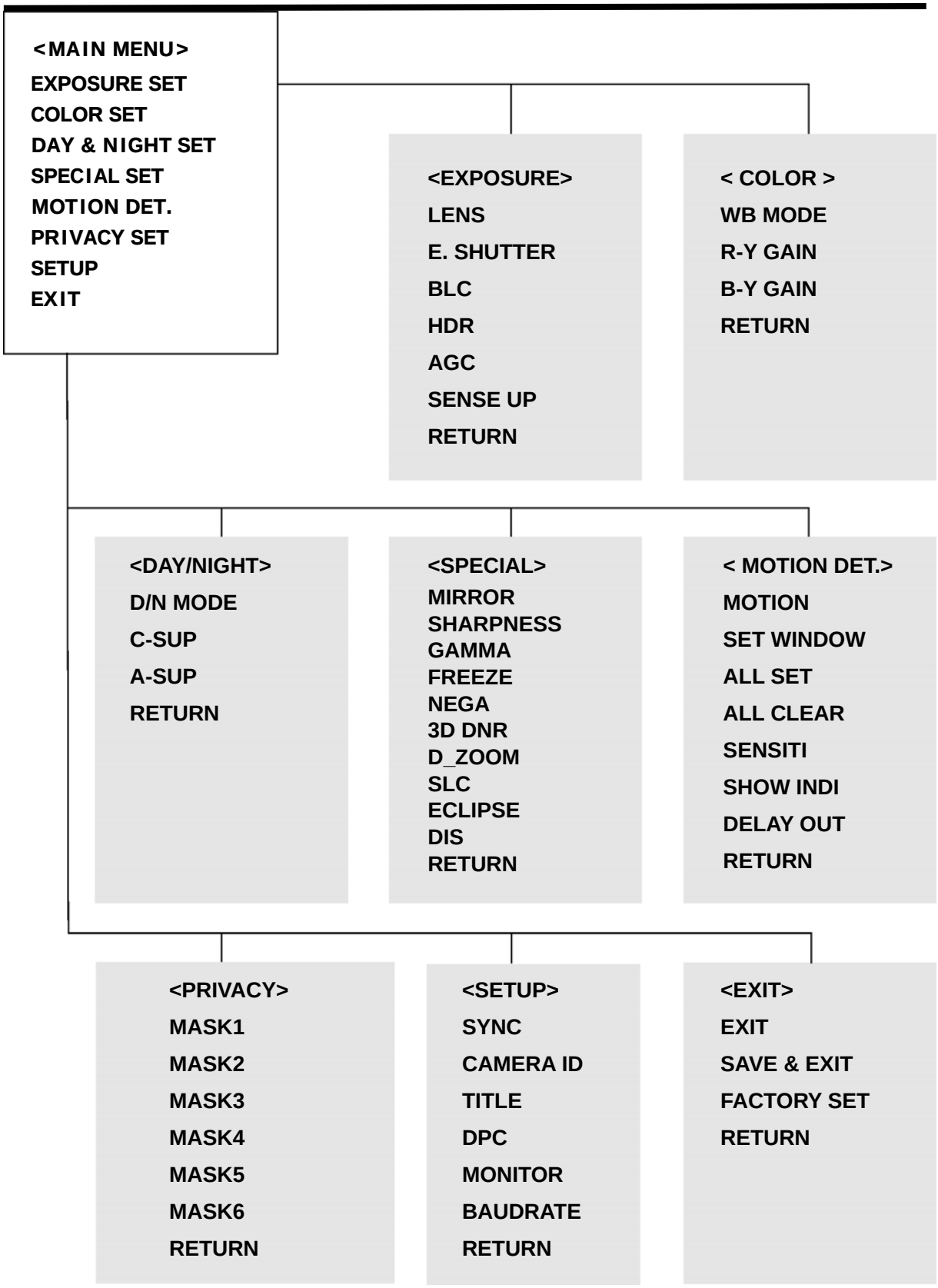
Final Installation

When all connections are made, secure the front plate to the base plate using the security screws previously removed using no. 20 Torx bit.

OSD Menu for Analog Camera

Settings can be made using the contact switch on the plug in controller.

CAMERA OPERATION WITH OSD



OSD MAIN SCREEN

All OSD operation is via the contact switch on the plug in controller.

[CENTER]	**Turn OSD menu ON or to go into Sub Menu**
[UP] / [DOWN]	**UP or DOWN of Cursor**
[LEFT] / [RIGHT]	**Change setting**

<EXPOSURE SET>

Press the **[ENTER]** button to access the **"EXPOSURE SET"** mode.

1) LENS: Select the type of lens. (This camera has a fixed lens.)

MANUAL: Select when fixed lens is used.

Sub Menu - MANUAL Level adjustment

(Adjust brightness of fixed lens.)

DC: Select when DC Varifocal lens is used.

Sub Menu - DC Level adjustment

(Adjust brightness of varifocal lens.)

2) E. SHUTTER: Electronic Shutter setting

Able to set from 256 to 1/100000 (Shutter speed adjustment)

Change FLK MODE (Select when using flicker mode.)

3) BLC: Backlight Compensation can be turned ON or OFF (default).

Select BLC ON/OFF (Backlight compensation function)

Sub Menu - Set BLC activity area

4) HDR: The dynamic range can be turned ON or OFF (default).

Select HDR ON/OFF (Similar function as WDR)

Sub Menu - Adjust HDR level

5) AGC: Automatic Gain Control can be set to LOW, MEDIUM, HIGH or OFF.

Select AGC OFF / LOW / MIDDLE / HIGH

6) SENSE UP: Sense Up can be set to X2 to X256 (X4 is default) or turned OFF.

When it is on, the camera controls sensitivity as it automatically detects the light level in dark environments and maintains a clear picture.

7) RETURN: Return to Main menu.

<COLOR SET>

Press the **[ENTER]** button to access the **"COLOR SET"** mode

1) WB MODE: The White Balance provides settings of AWC (default), ATW, Manual or Push Lock.

Select AWC/ATW/MANUAL/PUSH LOCK (adjust white balance).

Select MANUAL WB (Manual white balance mode).

Sub Menu -Select M.WB R (Adjust Red level when using manual WB).

Sub Menu -Select M.WB B (Adjust Blue level when using manual WB).

2) R-Y GAIN: Adjust RED gain.

3) B-Y GAIN: Adjust BLUE gain.

4) RETURN: Return to Main menu.

<DAY & NIGHT SET>

Press the **[ENTER]** button to access the **"DAY & NIGHT SET"** mode

1) D&N MODE: DAY & NIGHT Setting

Select AUTO/COLOR/BW/EXT

(TDN FUNCTION/COLOR/BLACK AND WHITE)

AUTO: The camera automatically switches between day and night.

BURST: Burst ON / OFF Setting (Only removing burst signal)

COLOR ► BW: Switching time setting

BW ► COLOR: Switching time setting

READ TIME: Read Time setting (Adjust filter switching time)

RETURN

COLOR: The camera stays in day mode (default).

B/W: The camera stays in night mode.

EXT: The camera stays in external mode.

2) C-SUP: Color Suppress Setting.

3) A-SUP: Aperture suppress setting.

4) RETURN: Return to Main menu.

<SPECIAL SET>

Press the **[ENTER]** button to access the **"SPECIAL SET"** mode

1) MIRROR: OFF/MIRROR/V_FLIP/ROTATE. Selectable (left&right/up&down/rotate)

2) SHARPNESS: Adjust Sharpness (Image sharpness can be adjusted)

3) GAMMA: GAMMA Setting. Select 0.45/0.6/1.0 (Adjust gamma level)

4) FREEZE: Image freeze function

5) NEGA.: Y Signal, Color Reverse function

6) 3D DNR: 3D DNR OFF/LOW/MIDDLE/HIGH Setting

(Adjust NOISE when low light condition)

7) D_ZOOM: D_ZOOM ON/OFF Setting.

Adjustable from X1.0 to X3.0

Change left/right, up/down. Show ZOOM,PAN,TILT amount (shows on the right side of the bottom)

8) SLC: Side Light Compensation can adjust the brightness of the image in the corners of the screen. It can be turned ON or OFF (default). ON allows settings of 0-50.

9) ECLIPSE: Highlight Mask Exposure is ON or OFF (default) selectable.

Eclipse Level Setting (Brightness of Eclipse is adjustable)

10) DIS: DIS ON/OFF Setting (Digital Image Stabilization)

11) RETURN: Return to Main menu.

<MOTION DET.>

Press the **[ENTER]** button to access the **"MOTION DET."** Mode

1) MOTION: Motion ON/OFF Setting

2) SET WINDOW: Set the range when using motion detection function.

Set the screen range for motion detection. (240 cells can be selected or deselected)

This feature allows you to detect the movement of an object in 240 different areas of the screen and display an alarm on the screen.

3) ALL SET: Set entire screen as a range for motion.

4) ALL CLEAR: Cancel entire screen range setting for motion.

5) SENSITI.: Adjust sensitivity when using motion detection.

As the sensitivity level increases, smaller movements are detected

6) SHOW INDI.: Motion defected indicator can be selected as OFF / ICON / TRACE

7) DELAY OUT: Alarm signal display on the screen is delayed from 1sec to 15sec

8) RETURN: Return to Main menu.

<PRIVACY SET>

Press the **[ENTER]** button to access the **"PRIVACY SET"** Mode

1) MASK1: MASK1 Screen setting

2) MASK2: MASK2 Screen setting

3) MASK3: MASK3 Screen setting

4) MASK4: MASK4 Screen setting

5) MASK5: MASK5 Screen setting

6) MASK6: MASK6 Screen setting

7) RETURN: Return to Main menu.

Select MASK1~6 (Set from 1 to 6 where wish to be hidden). Mask Range can be adjusted; can set in different

shapes. Mask color setting (Can change the color of hidden part).

This function sets certain areas of the screen to be hidden.

The image is divided into 6 zones.

<SETUP>

Press the **[ENTER]** button to access the **"SETUP"** Mode.

1) SYNC: Sync Setting

Line Lock Mode Setting (Select when using line lock)

RANGE SETTING (Set line lock range)

2) CAMERA ID: Camera ID Setting (Set a camera ID no. as a unique identifier.)

3) TITLE: Title ON/OFF Setting

Title EDIT (Select desired characters using joystick)

Title Reset (Clears the title)

Title Position Select

4) DPC: DPC Auto Setting (Dead pixels are automatically removed)

WHITE THR. (Cancelling White defective pixels)

BLACK THR. (Cancelling Black defective pixels)

DPC Level gain setting (Overall level can be adjusted)

5) MONITOR: Monitor Setting Mode (CRT/LCD Selectable)

<EXIT>

Press the **[ENTER]** button to access the **"EXIT"** Mode

1) EXIT

2) SAVE & EXIT: OSD menu after saving current setting.

3) FACTORY SET: Go back to factory default.

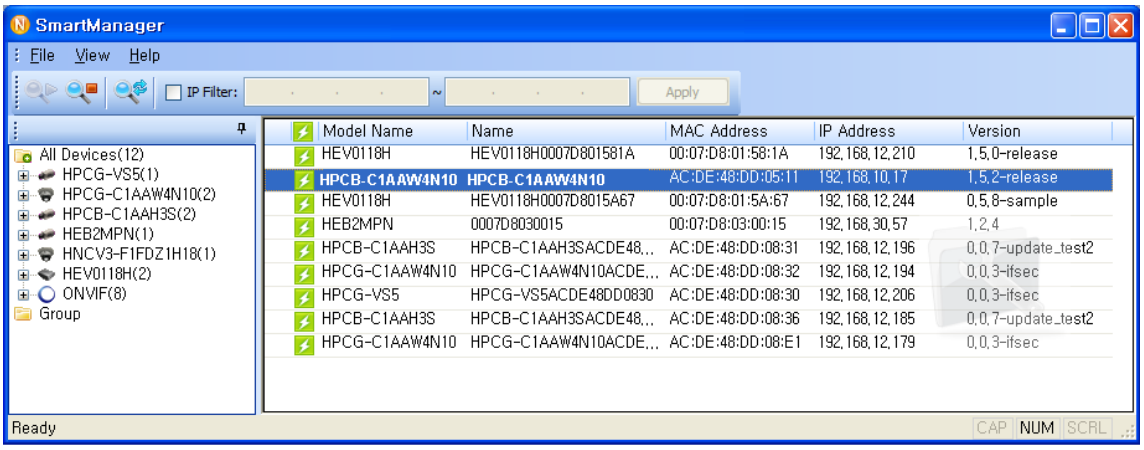
4) RETURN: Return to Main menu

2.5 Network Connection and IP assignment

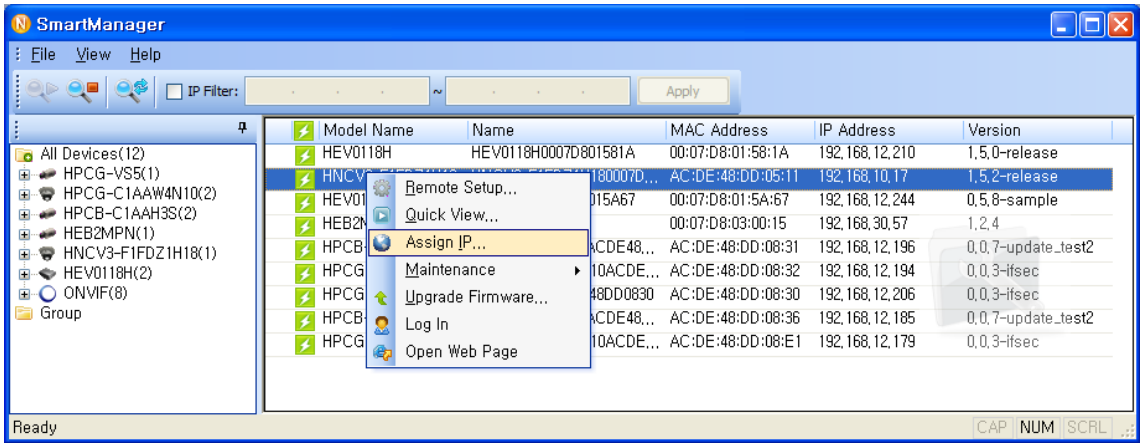
The V-CELL-IP camera is designed for use on an Ethernet network and requires an IP address for access. Most networks today have a DHCP server that automatically assigns IP addresses to connected devices. By the factory default, your camera is set to obtain the IP address automatically via DHCP server. If your network does not have a DHCP server the network camera will use 192.168.1.100 as the default IP address.

If DHCP is enabled and the product cannot be accessed, run the “Smart Manager” utility on the CD to search and allocate an IP address to your products, or reset the product to the factory default settings and then perform the installation again.

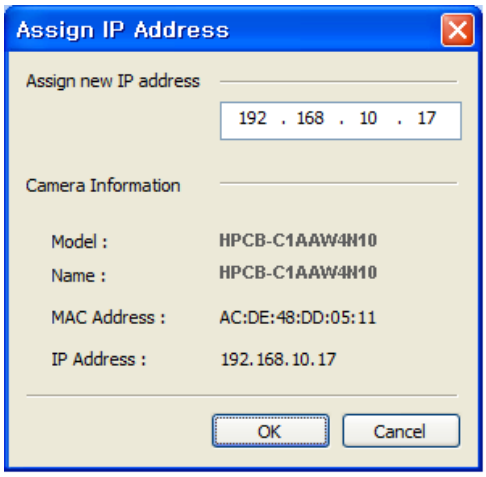
1. Connect the Network Camera/device to the network and power up.
2. Start SmartManager utility (All programs > NautilusClient16 > SmartManager), the main window will be displayed, after a short while any network devices connected to the network will be displayed in the list.


SmartManager
File View Help
IP Filter:
Apply
All Devices(12)
HPCG-VS5(1)
HPCG-C1AAW4N10(2)
HPCB-C1AAH3S(2)
HEB2MPN(1)
HNCV3-F1FDZ1H18(1)
HEV0118H(2)
ONVIF(8)
Group
Model Name | Name | MAC Address | IP Address | Version
HEV0118H | HEV0118H0007D801581A | 00:07:D8:01:58:1A | 192,168,12,210 | 1,5,0-release
HPCB-C1AAW4N10 | HPCB-C1AAW4N10 | AC:DE:48:DD:05:11 | 192,168,10,17 | 1,5,2-release
HEV0118H | HEV0118H0007D8015A67 | 00:07:D8:01:5A:67 | 192,168,12,244 | 0,5,8-sample
HEB2MPN | 0007D8030015 | 00:07:D8:03:00:15 | 192,168,30,57 | 1,2,4
HPCB-C1AAH3S | HPCB-C1AAH3SACDE48,.. | AC:DE:48:DD:08:31 | 192,168,12,196 | 0,0,7-update_test2
HPCG-C1AAW4N10 | HPCG-C1AAW4N10ACDE,.. | AC:DE:48:DD:08:32 | 192,168,12,194 | 0,0,3-ifsec
HPCG-VS5 | HPCG-VS5ACDE48DD0830 | AC:DE:48:DD:08:30 | 192,168,12,206 | 0,0,3-ifsec
HPCB-C1AAH3S | HPCB-C1AAH3SACDE48,.. | AC:DE:48:DD:08:36 | 192,168,12,185 | 0,0,7-update_test2
HPCG-C1AAW4N10 | HPCG-C1AAW4N10ACDE,.. | AC:DE:48:DD:08:E1 | 192,168,12,179 | 0,0,3-ifsec
Ready
CAP NUM SCRL

3. Select the camera on the list and click right button of the mouse. The pop-up menu displays as below.


SmartManager
File View Help
IP Filter:
Apply
All Devices(12)
HPCG-VS5(1)
HPCG-C1AAW4N10(2)
HPCB-C1AAH3S(2)
HEB2MPN(1)
HNCV3-F1FDZ1H18(1)
HEV0118H(2)
ONVIF(8)
Group
Model Name | Name | MAC Address | IP Address | Version
HEV0118H | HEV0118H0007D801581A | 00:07:D8:01:58:1A | 192,168,12,210 | 1,5,0-release
HPCB-C1AAW4N10 | HPCB-C1AAW4N10 | AC:DE:48:DD:05:11 | 192,168,10,17 | 1,5,2-release
HEV0118H | 015A67 | 00:07:D8:01:5A:67 | 192,168,12,244 | 0,5,8-sample
HEB2MPN | | 00:07:D8:03:00:15 | 192,168,30,57 | 1,2,4
HPCB-C1AAH3S | ACDE48,.. | AC:DE:48:DD:08:31 | 192,168,12,196 | 0,0,7-update_test2
HPCG-C1AAW4N10 | 10ACDE,.. | AC:DE:48:DD:08:32 | 192,168,12,194 | 0,0,3-ifsec
HPCG-VS5 | 48DD0830 | AC:DE:48:DD:08:30 | 192,168,12,206 | 0,0,3-ifsec
HPCB-C1AAH3S | ACDE48,.. | AC:DE:48:DD:08:36 | 192,168,12,185 | 0,0,7-update_test2
HPCG-C1AAW4N10 | 10ACDE,.. | AC:DE:48:DD:08:E1 | 192,168,12,179 | 0,0,3-ifsec
Remote Setup...
Quick View...
Assign IP...
Maintenance
Upgrade Firmware...
Log In
Open Web Page
Ready
CAP NUM SCRL

4. Select Assign IP. You cam see a Assign IP window. Enter the required IP address.



Note: For more information, refer to the Smart Manger User's Manual.

3. Operation

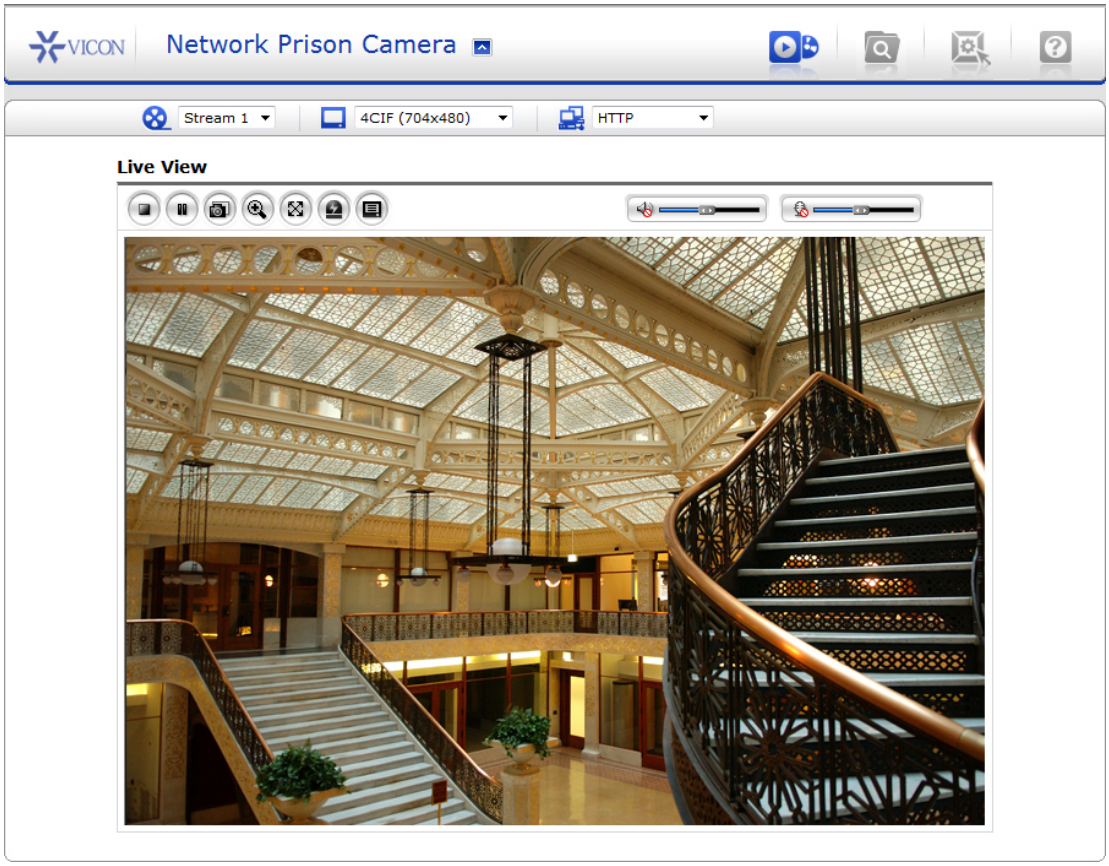
The V-CELL-IP Camera can be used with Windows® operating system and browsers. The recommended browsers are Internet Explorer®, Safari®, Firefox®, Opera and Google Chrome® with Windows.

Note: To view streaming video in Microsoft Internet Explorer, set your browser to allow ActiveX controls.
Note: Some screens may appear different (i.e., color scheme) depending on the firmware version, but the functionality is the same or similar.

3.1 Access from a browser

1. Start a browser (i.e., Internet Explorer).
2. Enter the IP address or host name of the Network Camera in the Location/Address field of your browser.
3. A starting page displays. Click Live View or Setup to enter web page.

4. The camera's **Live View** page appears in your browser.



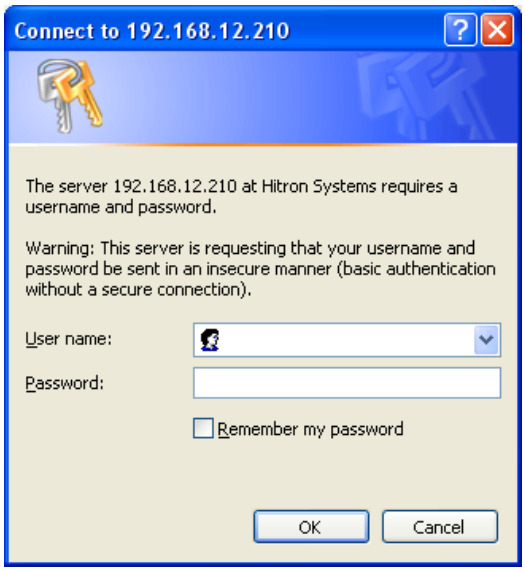
3.2. Access from the internet

Once connected, the V-CELL-IP Camera is accessible on your local network (LAN). To access the camera from the Internet you must configure your broadband router to allow incoming data traffic to the camera. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the camera. This is enabled from Setup > System > Network > NAT.

For more information, see NAT traversal (port mapping) for IPv4, on page 60.

3.3 Setting the admin password over a secure connection

To gain access to the product, the password for the default administrator user must be set. This is done in the “Admin Password” dialog, which is displayed when the network camera is accessed for the setup at the first time. Enter your admin name and password, set by the administrator.


Connect to 192.168.12.210
The server 192.168.12.210 at Hitron Systems requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

Note: The default administrator username is “ADMIN” and password is “1234”. If the password is lost, the Network Camera must be reset to the factory default settings. See “3.8 Resetting to the Factory Default Settings”.

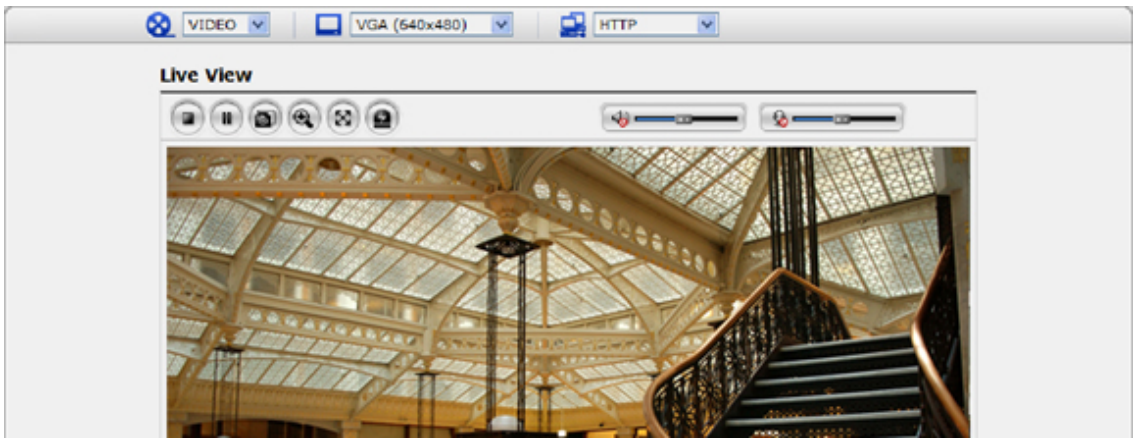
To prevent network eavesdropping when setting the admin password, this can be done via an encrypted HTTPS connection, which requires an HTTPS certificate (see note below).

To set the password via a standard HTTP connection, enter it directly in the first dialog shown below. To set the password via an encrypted HTTPS connection, see “3.5.4 System > Security > HTTPS”.

Note: HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate controls the encrypted exchange of information.

3.4 Live View Page

The live view page comes in several screen modes, including 704x480 (576), 640x480, 352x240 (288), and 320x240. Users select the most suitable one for their particular installation. Adjust the mode in accordance with your PC specifications and monitoring purposes.



1) General controls

Live View Page Search & Playback Page Setup Page Help Page

The video drop-down list allows you to select a customized or pre-programmed video stream on the live view page. Stream profiles are configured under Setup > Basic Configuration > Video & Image. See Basic Configuration, on page 26 for more information.

The resolution drop-down list allows you to select the most suitable video resolution to be displayed on Live View page.

The protocol drop-down list allows you to select which combination of protocols and methods to use, depending on your viewing requirements and on the properties of your network.

2) Control toolbar

The live viewer toolbar is available in the web browser page only. It displays the following buttons:

The Stop button stops the video stream being played. Pressing the key again toggles the start and stop. The Start button connects to the network camera or start playing a video stream.

The Pause button pauses the video stream being played.

The Snapshot button takes a snapshot of the current image. The location where the image is saved can be specified.

The digital zoom activates a zoom-in or zoom-out function for video image on the live screen.

The Full Screen button causes the video image to fill the entire screen area. No other windows will be visible. Press the 'Esc' button on the computer keyboard to cancel full screen view.

The Manual Trigger button activates a pop-up window to manually start or stop the event.

The Camera Menu button activates a pop-up window for camera menu control.

Use this scale to control the volume of the speakers.

Use this scale to control the volume of the microphone.

Use this scale to control the volume of the speakers and microphones.

3) Video Streams

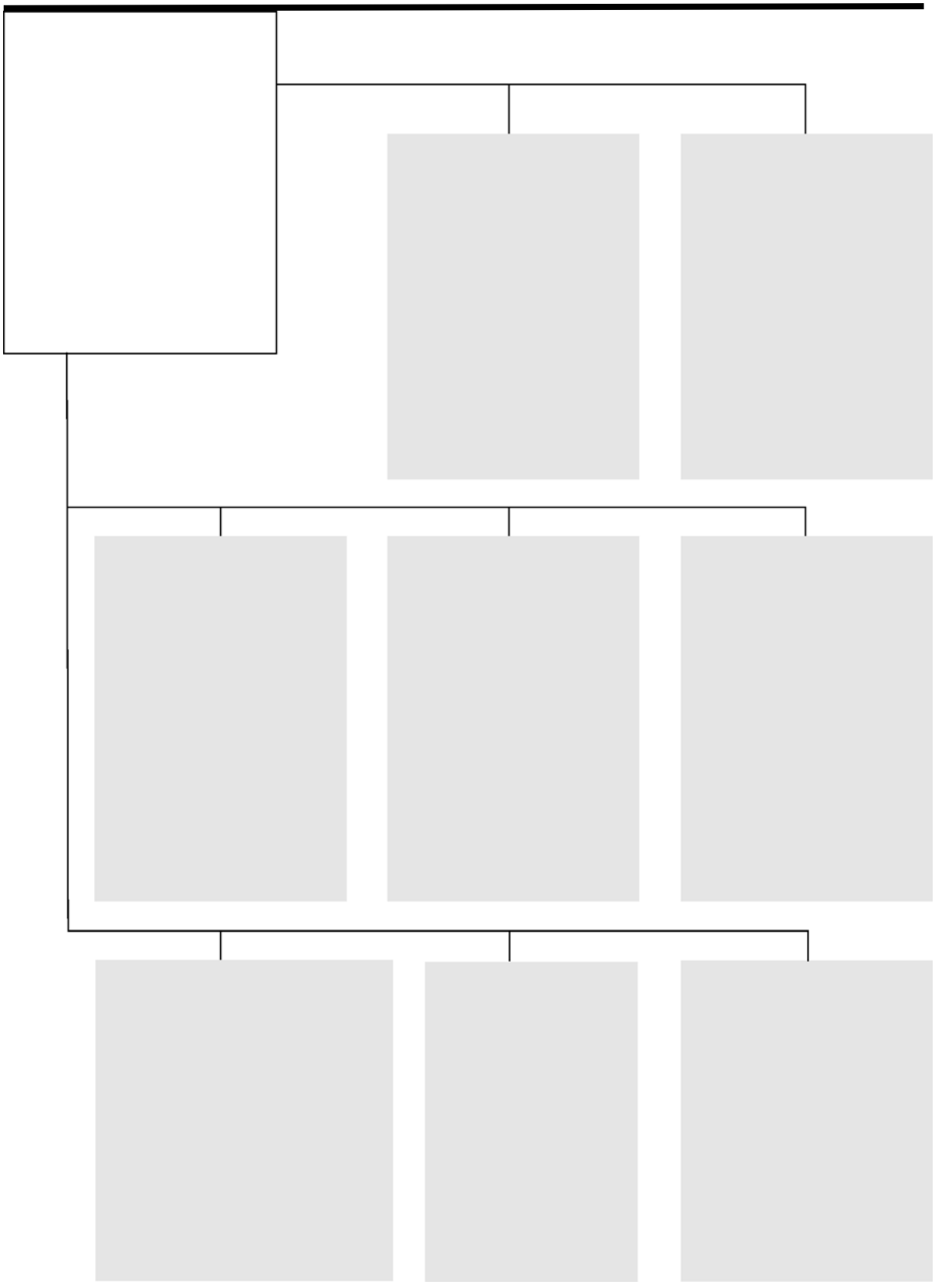
The Network Camera provides several images and video stream formats. Your requirements and the properties of your network will determine the type you use.

The Live View page in the Network Camera provides access to H.264, MPEG-4 and Motion JPEG video streams, and to the list of available video streams. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

4) Camera Setup

Settings can be made using the virtual keypad of the camera menu toolbar in the live view page or contact switch on the plug in controller. For an explanation of terms, refer to analog section.

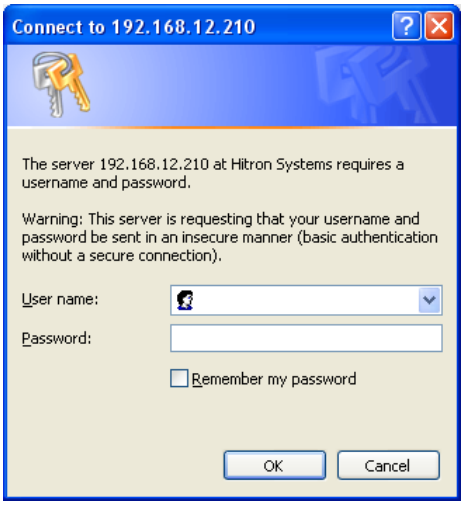
CAMERA OPERATION WITH O.S.D.



3.5 Network Camera Setup

This section describes how to configure the V-CELL-IP Camera. It is intended for Administrators, who have unrestricted access to all the Setup tools, and Operators, who have access to the settings for Basic, Live View, Video & Image, Event, and System Configuration.

You can configure the V-CELL-IP Camera by clicking Setup in the top right-hand corner of the Live View page. Click on this page to access the online help that explains the Setup tools.


Connect to 192.168.12.210
The server 192.168.12.210 at Hitron Systems requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

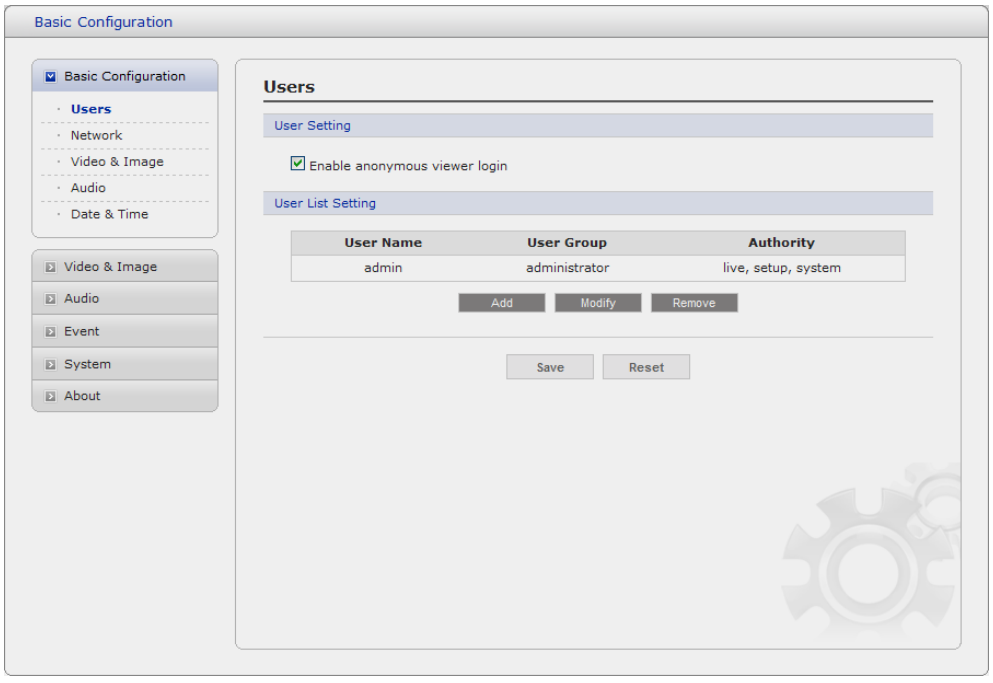
When accessing the Network Camera for the first time, the “Admin Password” dialog appears. Enter your admin name and password, set by the administrator.

Note: If the password is lost, the Network Camera must be reset to the factory default settings. See “3.8 Resetting to the Factory Default Settings.”

3.5.1 Basic Configuration

1) Users

User access control is enabled by default. An administrator can set up other users, by giving these user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page, as described below:



The **user list** displays the authorized users and user groups (levels):

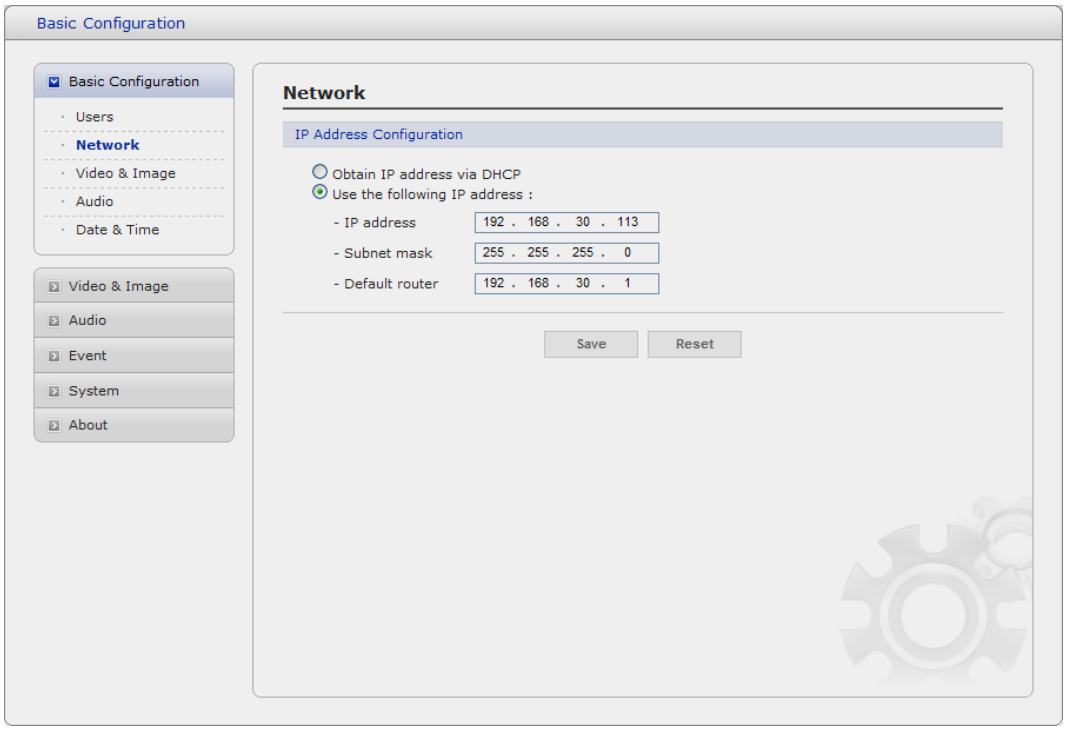
User Group	Authority
Guest	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has unrestricted access to the Setup tools and can determine the registration of all other users.

An administrator can Add, Modify or Remove users in the list by clicking lthe appropriate button. Click Save to save the settings or Reset to cancel.

- **Enable anonymous viewer login:** Check the box to use the webcasting features. Refer to "3.5.2 Video & Image" for more details.

2) Network

The Network Camera supports both IP version 4 and IP version 6. Both versions may be enabled simultaneously, and at least one version must always be enabled. When using IPv4, the IP address for the video camera can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the video cameras receive an IP address according to the configuration in the network router. There is also the option of using the Internet Dynamic DNS Service. For more information on setting the Network, see Setup> System>Security>Network.



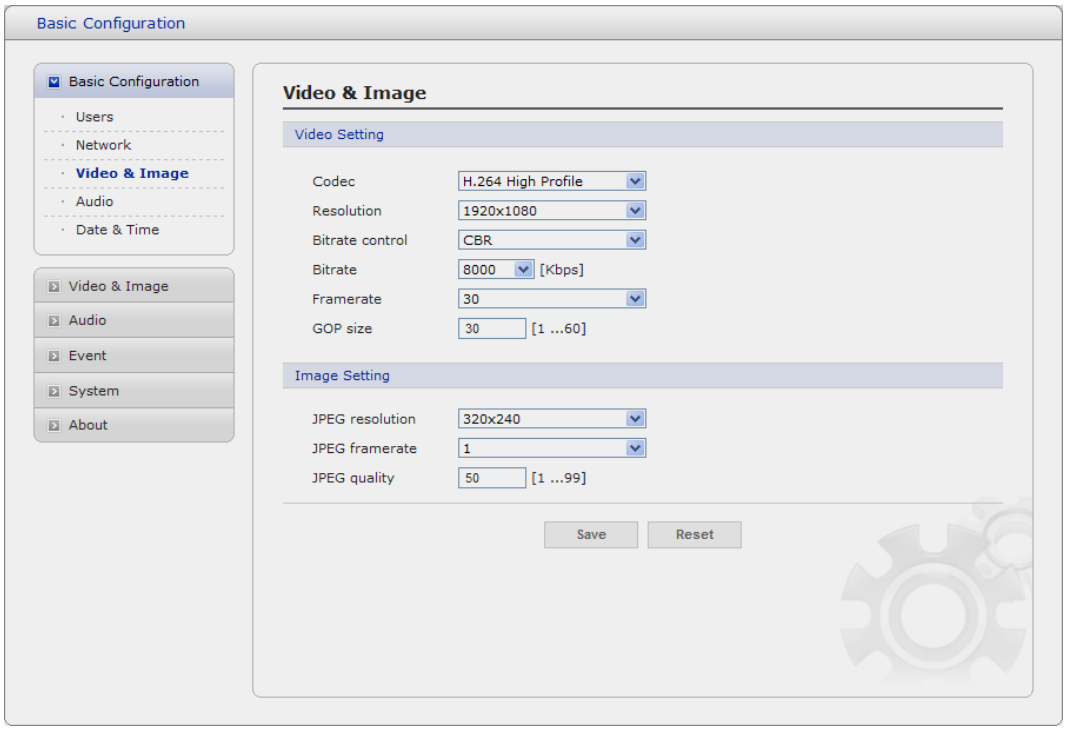
- **Obtain IP address via DHCP** - Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.
- **Use the following IP address** - To use a static IP address for the Network Camera, check the radio button and then make the following settings:
  - **IP address:** Specify a unique IP address for your Network Camera.

- **Subnet mask:** Specify the mask for the subnet the Network Camera is located on.
- **Default router:** Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

Notes:

1. DHCP should only be enabled if using dynamic IP address notification, or if your DHCP server can update a DNS server, which then allows you to access the Network Camera by name (host name). If DHCP is enabled and you cannot access the unit, you may have to reset it to the factory default settings and then perform the installation again.
2. The ARP/Ping service is automatically disabled two minutes after the unit is started, or as soon as an IP address is set.
3. Pinging the unit is still possible when this service is disabled.

3) Video & Image



- **Video Setting**
  - **Codec:**

    The codec settings are separated into MPEG-4 and H.264.

    H.264 is also known as MPEG-4 Part 10. This is the new generation compression standard for digital video. This function offers higher video resolution than Motion JPEG or MPEG-4 at the same bit rate and bandwidth, or the same quality video at a lower bit rate.

    Profile:

    There are 4 pre-programmed stream profiles available for quick set-up.

    Choose the form of video encoding you wish to use from the drop-down list:

* **H.264 MP (Main Profile):**
  Primarily for low-cost applications that require additional error robustness, this profile is rarely used in videoconferencing and mobile applications; it does add additional error resilience tools to the Constrained Baseline Profile. The importance of this profile is fading after the Constrained Baseline Profile has been defined.
* **H.264 BP (Base Profile):**
  Originally intended as the mainstream consumer profile for broadcast and storage applications, the importance of this profile faded when the High Profile was developed for those applications.
* **MPEG4 SP (Simple Profile):**
  Mostly aimed for use in situations where low bit rate and low resolution are mandated by other conditions of the applications, like network bandwidth, device size etc.
* **MPEG4 ASP (Advanced Simple Profile):**
  Its notable technical features relative to the Simple Profile, which is roughly similar to H.263, include "MPEG"-style quantization, interlaced video, B pictures (also known as B Frames), Quarter Pixel motion compensation (Qpel), and Global motion compensation (GMC).

- **Resolution:**
  Enables users to determine a basic screen size when having an access through the Web Browser or PC program. The screen size control comes in seven modes like 640x480, 352x240(288), and 320x240. Users can reset the selected screen size anytime while monitoring the screen on a real-time basis.

- **Bitrate control:**
  Limiting the maximum bit rate helps control the bandwidth used by the H.264 or MPEG-4 video stream. Leaving the Maximum bit rate as unlimited maintains consistently good image quality but increases bandwidth usage when there is more activity in the image. Limiting the bit rate to a defined value prevents excessive bandwidth usage, but images are lost when the limit is exceeded.

  Note that the maximum bit rate can be used for both variable and constant bit rates.

  The bit rate can be set as Variable Bit Rate (VBR) or Constant Bit Rate (CBR). VBR adjusts the bit rate according to the image complexity, using up bandwidth for increased activity in the image, and less for lower activity in the monitored area.

  CBR allows you to set a fixed target bitrate that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity (but in this case cannot), the frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either the frame rate or the image quality whenever the bit rate needs to be increased. Not setting a priority means the frame rate and image quality are equally affected.

- **Frame rate:**
  Upon the real-time play, users should select a frame refresh rate per second. If the rate is high, the image will become smooth. On the other hand, if the rate is low, the image will not be natural but it can reduce a network load.

- **GOP size:**
  Select the GOP (Group of Picture) size. If users want to have a high quality of fast images one by one, decrease the value. For the purpose of general monitoring, do not change a basic value. This may cause a problem to the system performance. Vicon recommends that GOP be the same as the fps.

• **Image Setting**

Sometimes the image size is large due to low light or complex scenery. Adjusting the frame rate and quality helps to control the bandwidth and storage used by the Motion JPEG video stream in these situations. Limiting the frame rate and quality optimizes bandwidth and storage usage, but may give poor image quality. To prevent increased bandwidth and storage usage, the Resolution, Frame rate, and Frame Quality should be set to an optimal value.

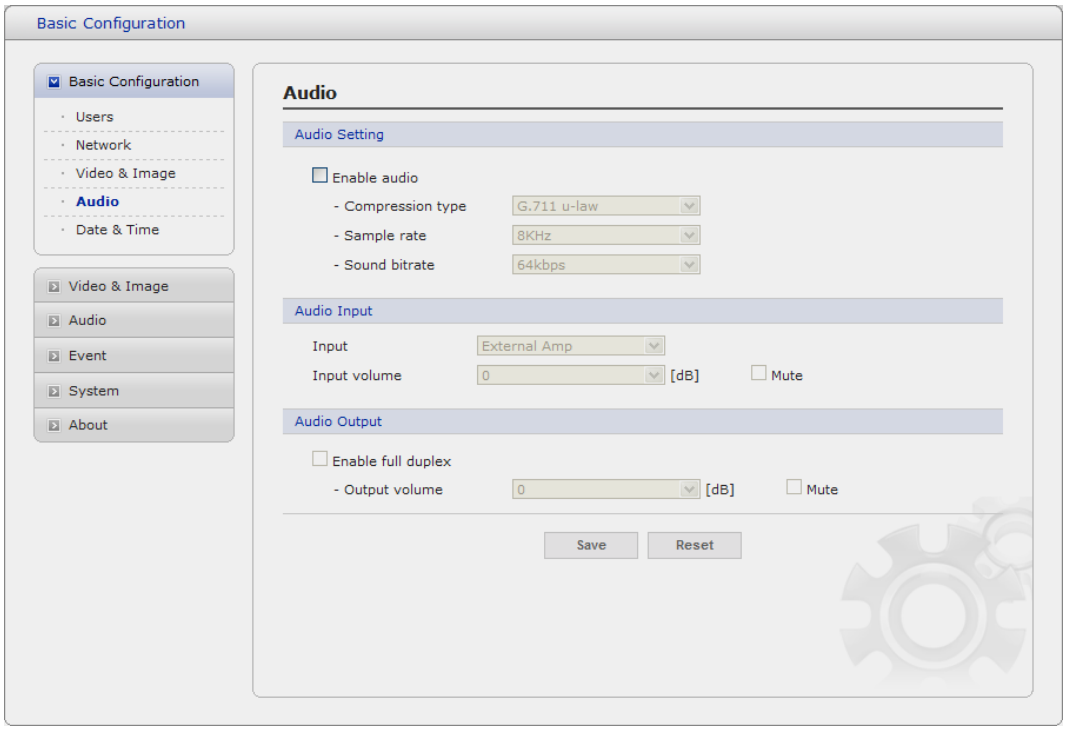
- **JPEG resolution:**
  Same as the video settings.

- **JPEG frame rate:**
  Same as the video settings.

- **JPEG quality:**
  Select the picture quality. If users want to have a high quality of fast images one by one, decrease the value. For the purpose of general monitoring, do not change a basic value. Such act may cause a problem to the system performance.

When satisfied with the settings, click **Save**, or click **Reset** to revert to previously saved settings.

4) Audio



The Network Camera can transmit audio to other clients using an external microphone and can play audio received from other clients by attaching a speaker. The Setup page has an additional menu item called **Audio**, which allows different audio configurations, such as, full duplex and simplex.

- **Audio Setting**
  - **Enable audio:**
    Check the box to enable audio in the video stream.

  - **Compression type:**
    Select the desired audio Compression format, G711. The “u-law” is for North America and Japan; the “a-law” if for Europe and the rest of the world.

  - **Sample rate:**
    Select the required Sample rate (number of times per second the sound is sampled). The higher the sample rate, the better the audio quality and the greater the bandwidth required.

  - **Sound bitrate:**
    Depending on the selected encoding, set the desired audio quality (bitrate). The settings affect the available bandwidth and the required audio quality.

- **Audio Input**
  Audio from an external line source can be connected to the I/O terminal of the network camera.
  - **Input volume:**
    If there are problems with the sound input being too low or high, it is possible to adjust the input gain for the microphone attached to the Network Camera.
- **Audio Output**
  - **Enable full duplex:**
    Check the box to enable Full Duplex mode. This means that you can transmit and receive audio (talk and listen) at the same time, without having to use any of the controls, like having a telephone conversation.

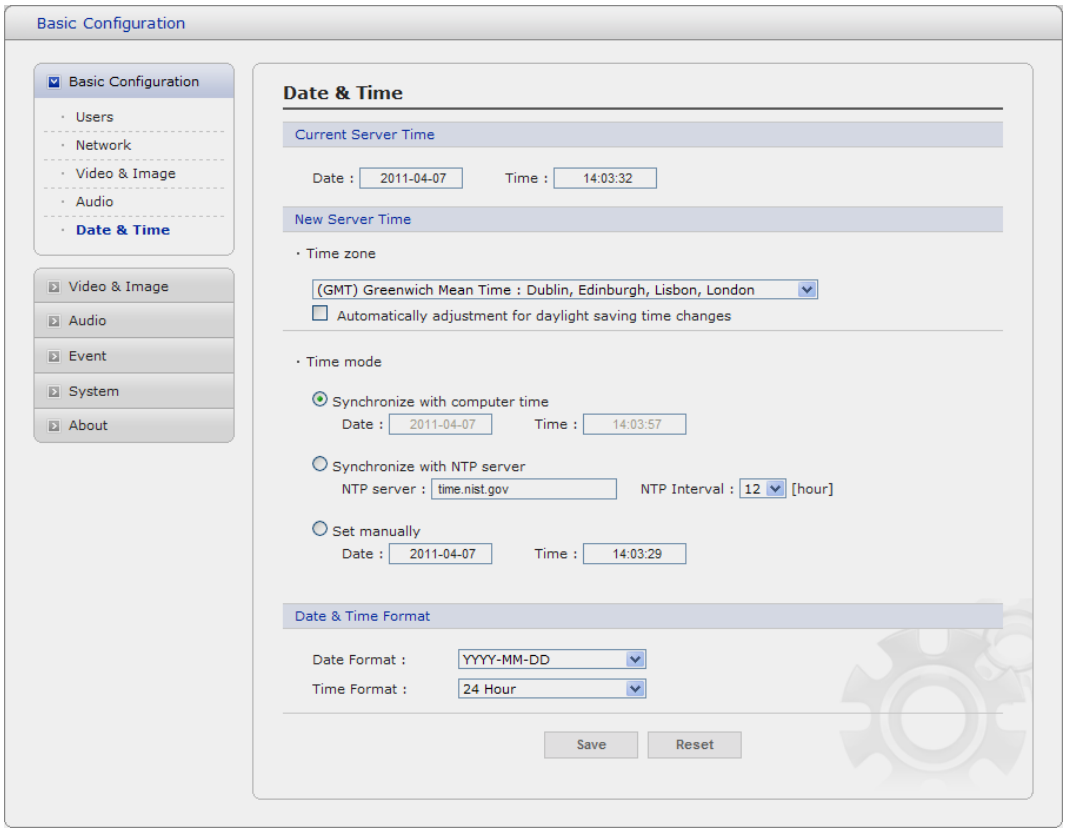
    Note: This mode requires that the client PC has a sound card with support for full-duplex audio.

    Uncheck the box Enable Simplex mode. The simplex mode only transmits audio from the Network Camera to any web client. It does not receive audio from other web clients.

  - **Output volume:**
    If the sound from the speaker is too low or high it is possible to adjust the output gain for the active speaker attached to the network camera.

When satisfied with the settings, click **Save**, or click **Reset** to revert to previously saved settings

5) Date & Time



- **Current Server Time**
  This displays the current date and time (24h clock). The time can be displayed in 12h clock format.

- **New Server Time**
  Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select the "Automatically adjustment for daylight saving time changes".

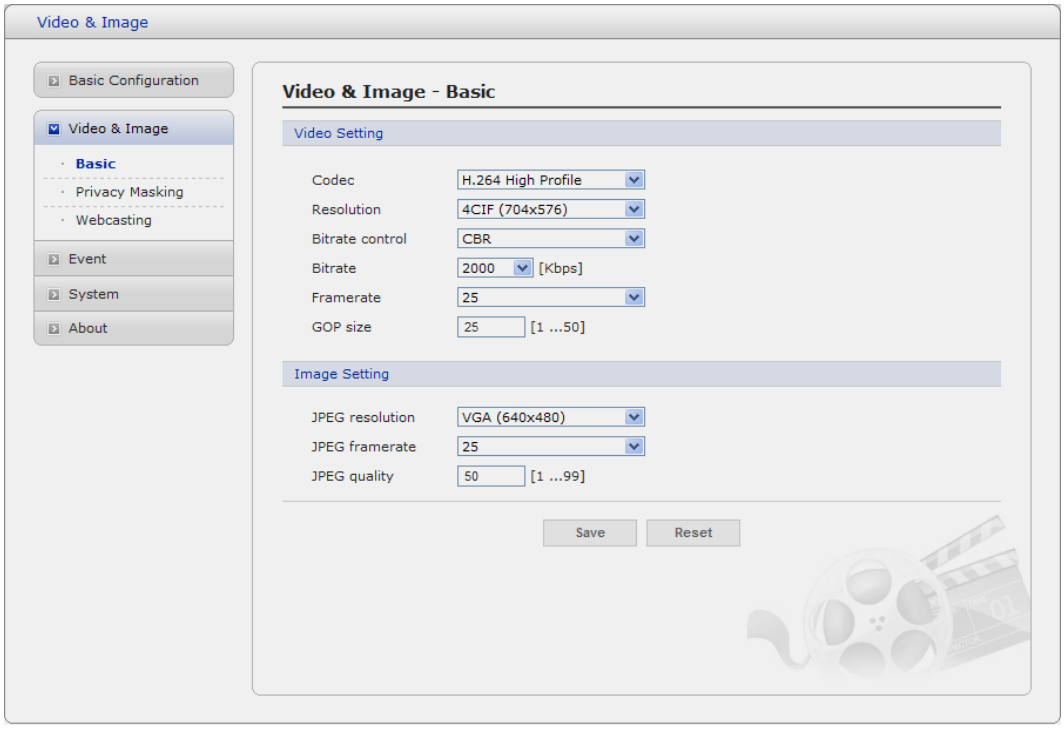
  From the **Time Mode** section, select the preferred method to use for setting the time:
  - **Synchronize with computer time:** sets the time from the clock on your computer.
  - **Synchronize with NTP Server:** the video camera will obtain the time from an NTP server every 60 minutes.
  - **Set manually:** this option allows you to manually set the time and date.

- **Date & Time Format**
  Specify the formats for the date and time (12h or 24h) displayed in the video streams.
  Select Date & Time format from the drop-down list.
  - **Date Format:** Specify the date format. YYYY: Year, MM: Month, DD: Day
  - **Time Format:** Specify the date format. 24 Hours or 12 Hours

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

3.5.2 Video & Image

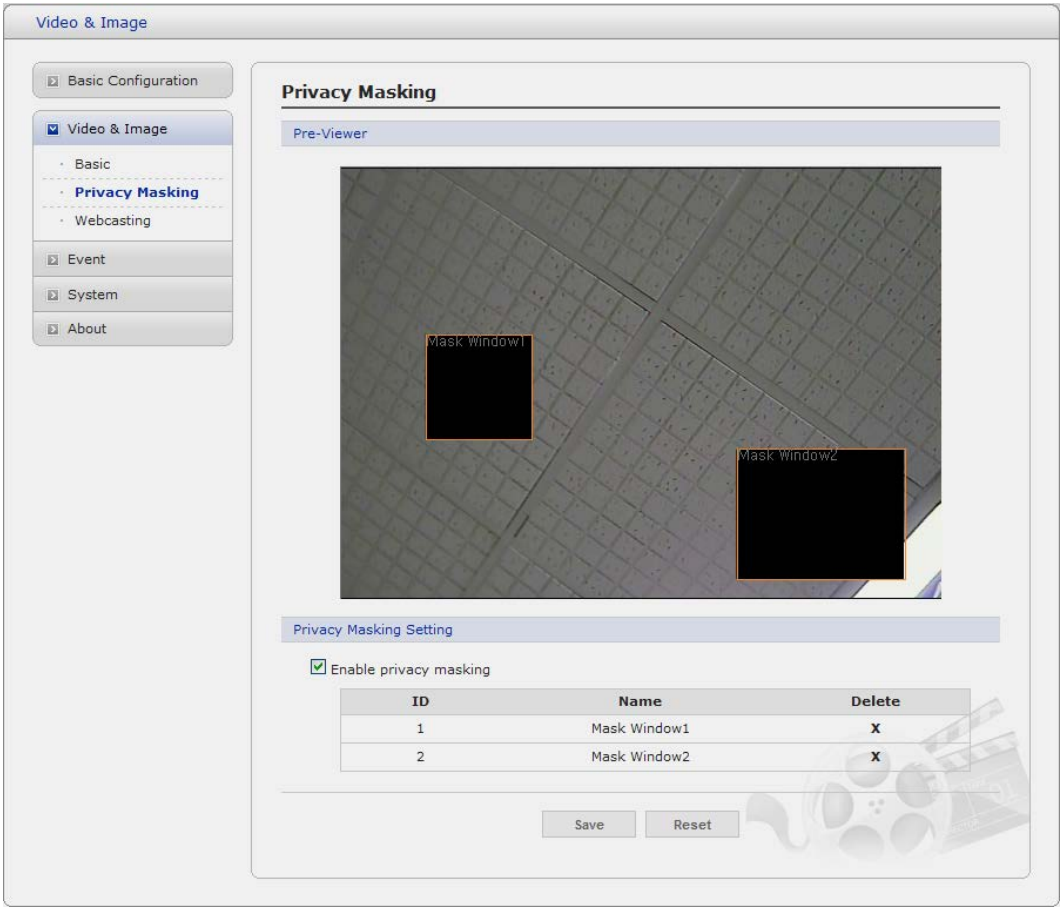
▼ Basic



Refer to “3.5.1 Basic Configuration > Video & Image” for more details.

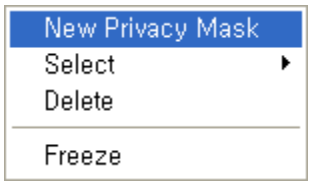
▼ Privacy Masking - Basic

The privacy masking function allows you to mask parts of the video image to be transmitted. You can set up to eight privacy masks; the color of privacy masks is black.



Select “Enable privacy masking” to activate the privacy masking function.

The privacy masks are configured by Mask windows. Each window can be selected by clicking with the mouse. It is also possible to **resize** or **delete,** or **move** the window by selecting the appropriate window at the mouse menu on the video screen.



To create a mask window, follow steps:

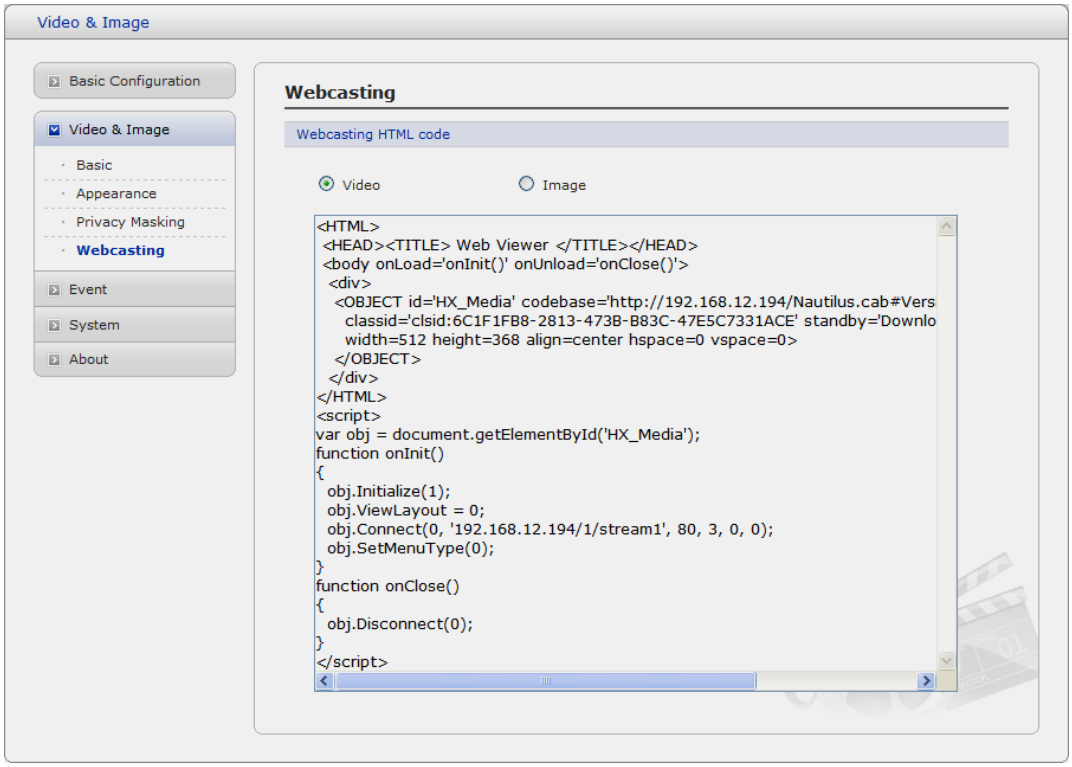
1. Click the right button of mouse to see the mouse menu.
2. Select New Privacy Mask in the mouse menu.
3. Click and drag mouse to designate a mask window area.

A mask window name can also be modified or deleted. Select a name and then modify items or select delete button.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

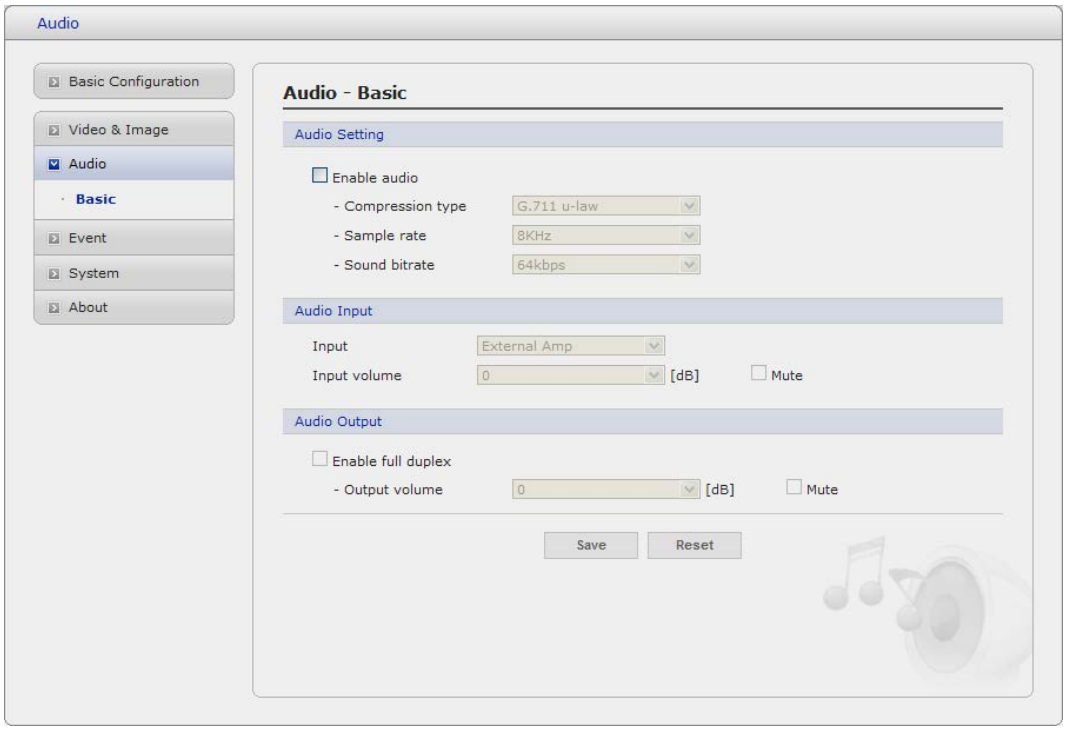
▼ Webcasting – Channel1

The Network Camera can stream live video to a website. Copy the HTML code generated on the screen and paste it in page code of the website you want to display live video.



Note: To use webcasting service, the Enable Anonymous viewer login option must be checked. Refer to “3.5.1 Basic Configuration > Users” for more details.

3.5.3 Audio

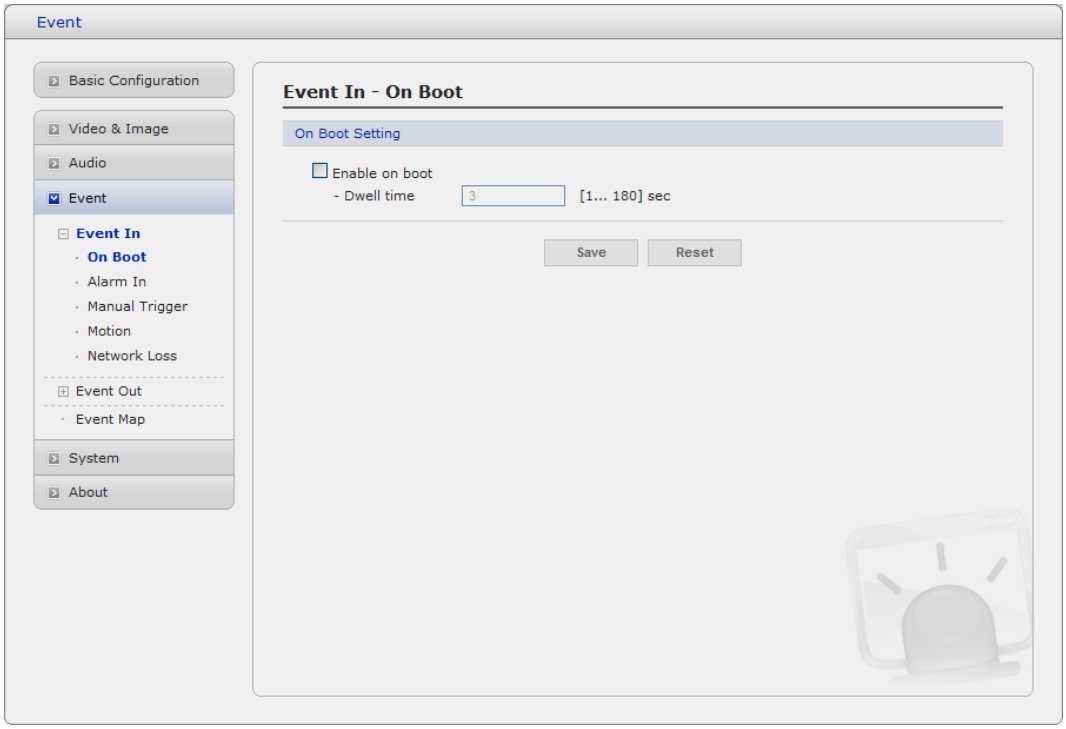


Refer to “3.5.1 Basic Configuration > Audio” for more details.

3.5.4 Event

1) Event-In

▼ On Boot

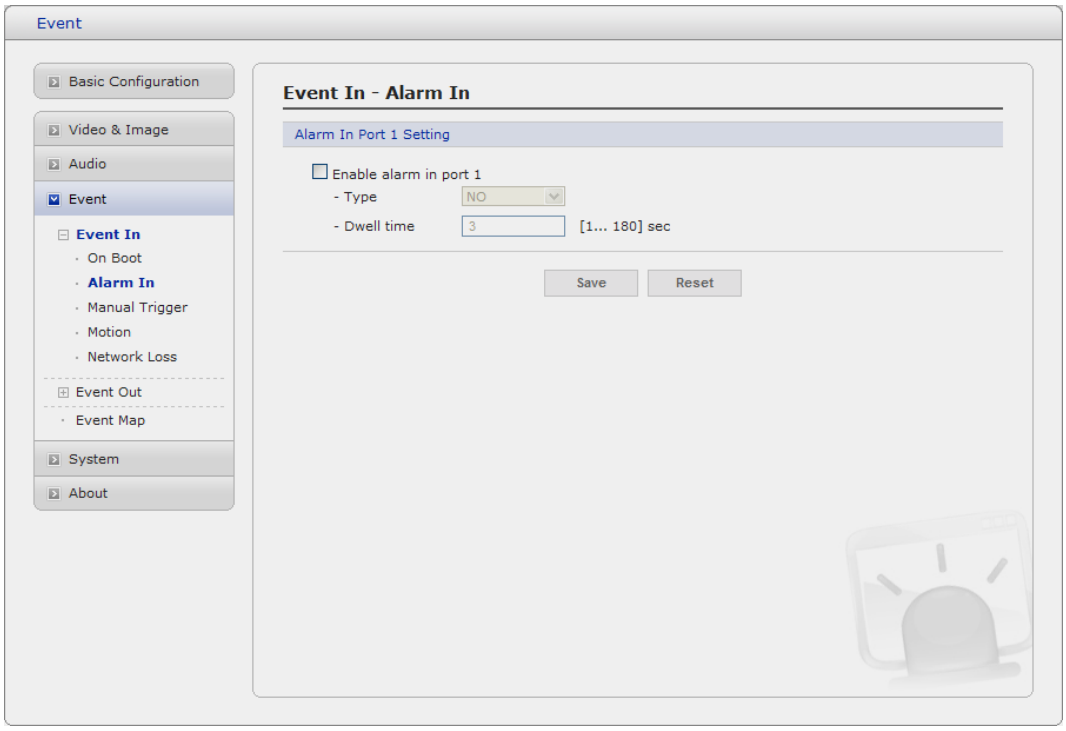


This is used to trigger the event every time the Network Transmitter is started. Select “Enable on boot” to activate the motion event.

Enter the Dwell time the event lasts from the point of detection, 1-180 seconds.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Alarm In

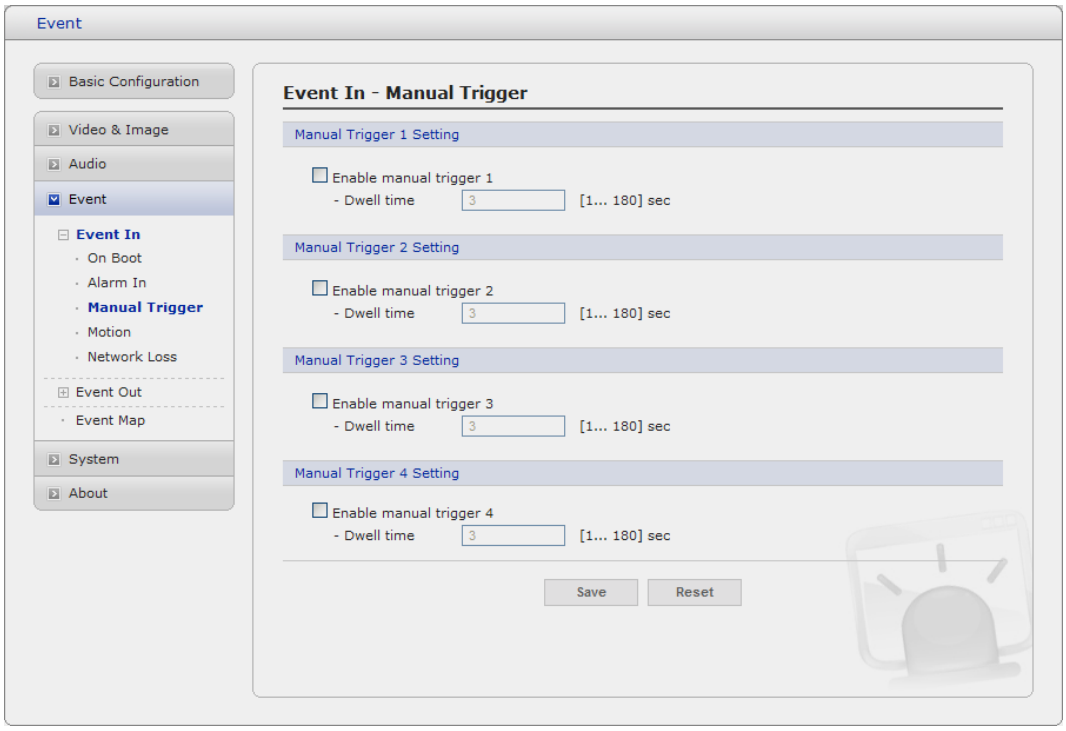


Select “Enable” to activate the alarm event. The Network Camera supports 1 alarm input port.

- **Type:** Choose the type of alarm you wish to use from the drop-down list.
- **Dwell Time:** Set the dwell time an event lasts for the specified alarm from the point of detection of an alarm input.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Manual Trigger



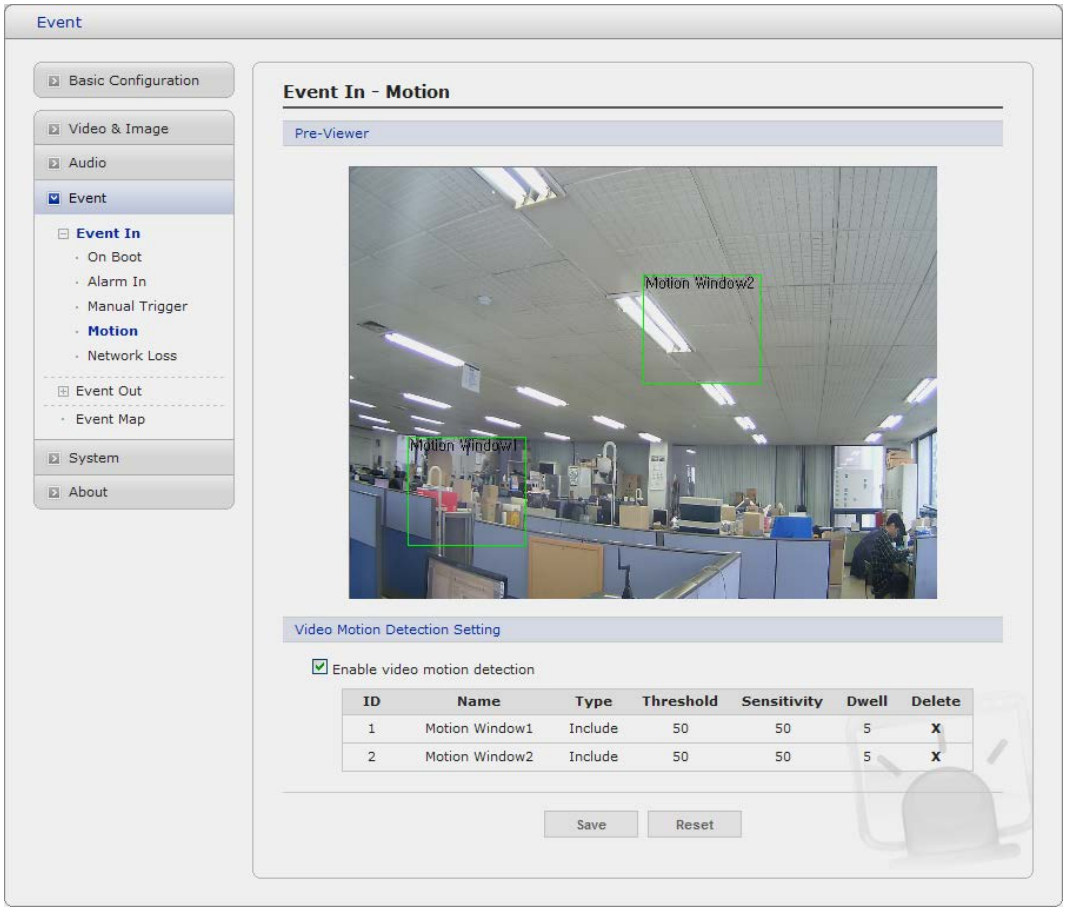
This option makes use of the manual trigger button provided on the live view page, which is used to start or stop the event type manually. Alternatively the event can be triggered via the product's API (Application Programming Interface).

Select “Enable manual trigger” to activate the manual trigger (for up to 4 manual triggers).

Set the dwell time the trigger lasts.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Motion



Select “Enable” to activate the motion window.

Motion detection is used to generate an alarm whenever movement occurs (or stops) in the video image. A total of 8 Motion and/or Mask windows can be created and configured.

Motion is detected in defined **Motion** windows, which are placed in the video image to target specific areas. Movement in the areas outside the motion windows will be ignored. If part of a motion window needs to be masked, this can be configured in a **Mask** window.

- **Pre-Viewer**
  Motion detection windows are configured by Motion or Mask windows. Each window can be selected by clicking with the mouse. It is also possible to **resize** or **delete,** or **move** the window by selecting the appropriate window at the mouse menu on the video screen.

To create a motion or mask window, follow steps:

1. Click the right button of mouse to see the mouse menu.
2. Select New Motion (or Mask) Window in the mouse menu.
3. Click and drag mouse to designate a motion area.

- **Motion Detection Setting**

  The behavior for each window is defined by adjusting the Threshold and Sensitivity, as described below.

  A motion index is a set of parameters describing Window Name, Type, Threshold, Sensitivity, and Dwell Time. Window Type is Include at the Motion, and Exclude at the Mask window.

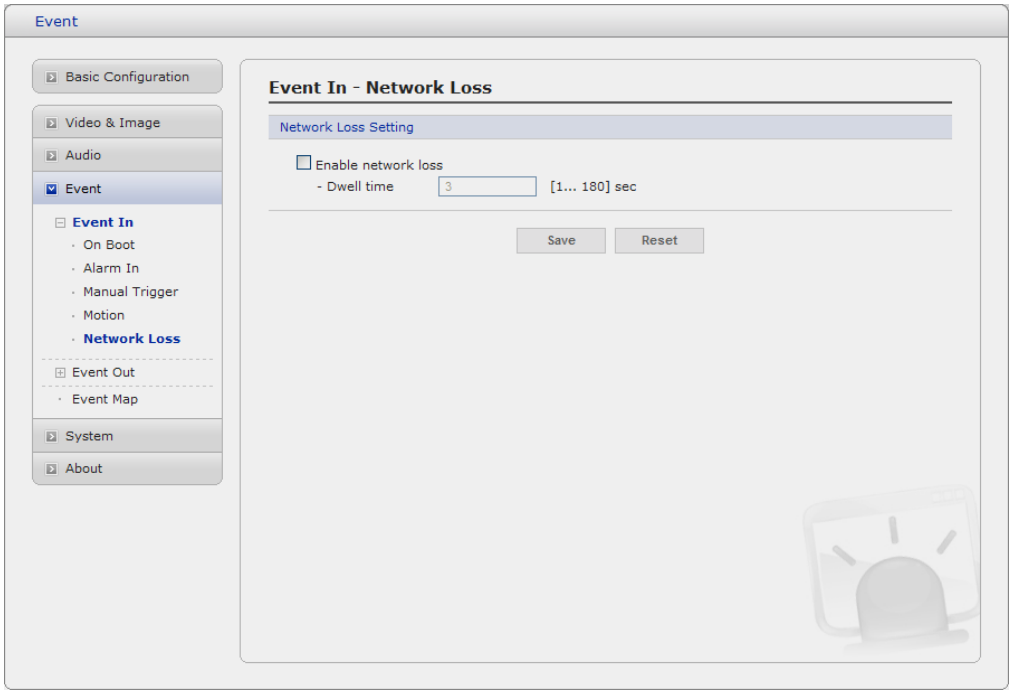
  - **Threshold:** Sets up the threshold for the motion detection. Threshold judges the amount of change in the area. Select from 1-100; a lower number increase frequency of alarms.
  - **Sensitivity:** Sets up the sensitivity for the motion detection. Sensitivity measures the level of motion in each motion area. Select from 1-100, 1 being the least sensitive to alarm condition.
  - **Dwell Time:** Set the hold time an event lasts from the point of detection of a motion (hold time).

  You can also modify or delete a motion index. It can be deleted using the table and modified by selecting it and changing parameters in the table. When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Network Loss

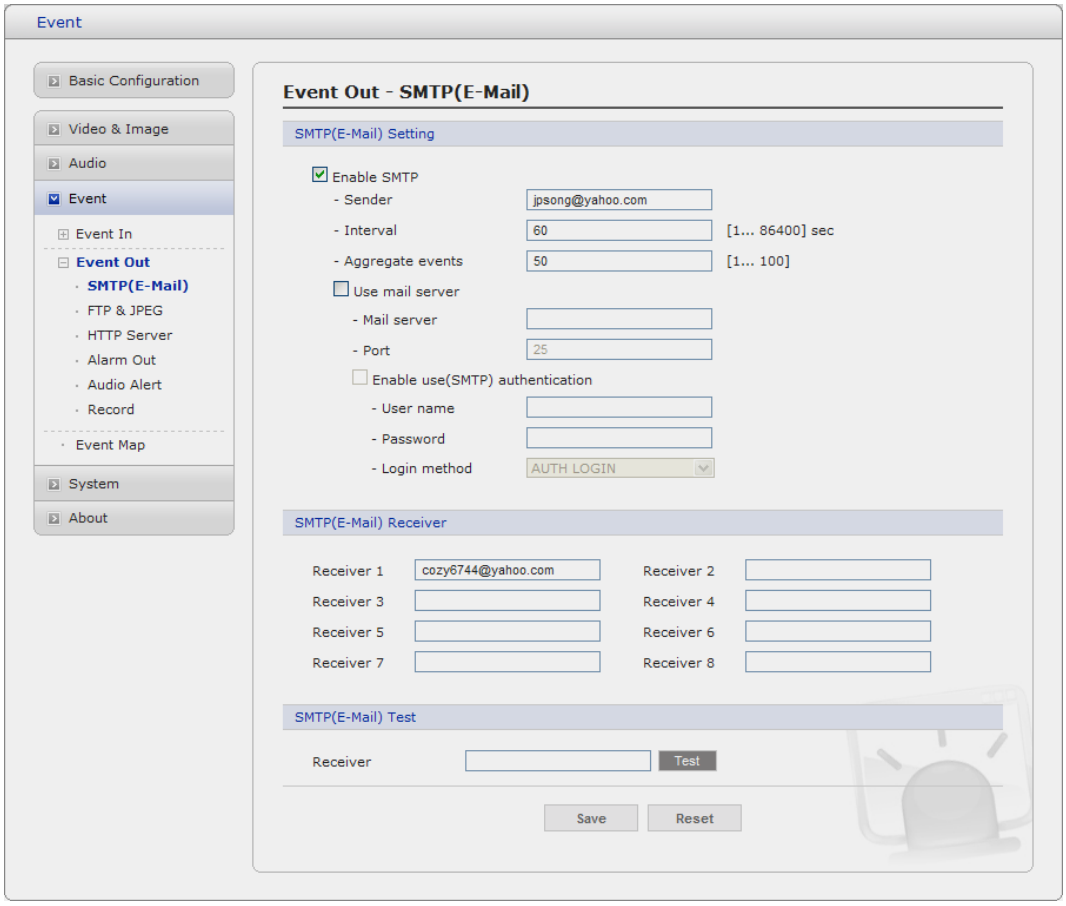
This is used to trigger the event every time the network connection fails. Select “Enable” to activate the Network Loss event. Select a dwell time for how long the event will last from the point of detection.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.



2) Event-Out

▼ SMTP (E-Mail)



The Network Camera can be configured to send event and error email messages via SMTP (Simple Mail Transfer Protocol).

- **SMTP (E-Mail) Setting**
  Select “Enable” to activate the SMTP operation.
  - **Sender:** Enter the email address to be used as the sender for all messages sent by the Network Transmitter.
  - **Interval:** Represents the frequency of the email notification when an event occurs.
  - **Aggregate events:** Shows the maximum number of emails sent within each interval.

Check the box to “Use mail server” if required.

- **Mail Server/Port:** Enter the host names (or IP addresses) and port numbers for your mail server in the fields provided to enable the sending of notifications and image email messages from the camera to predefined addresses via SMTP.

If your mail server requires authentication, check the box for Use authentication to log in to this server and enter the necessary information.

- **User Name/Password:** Enter the User Name and Password as provided by your network administrator or ISP (Internet Service Provider).

To ensure that the login procedure is performed as securely as possible when using SMTP authentication, you must define the weakest authentication method allowed.

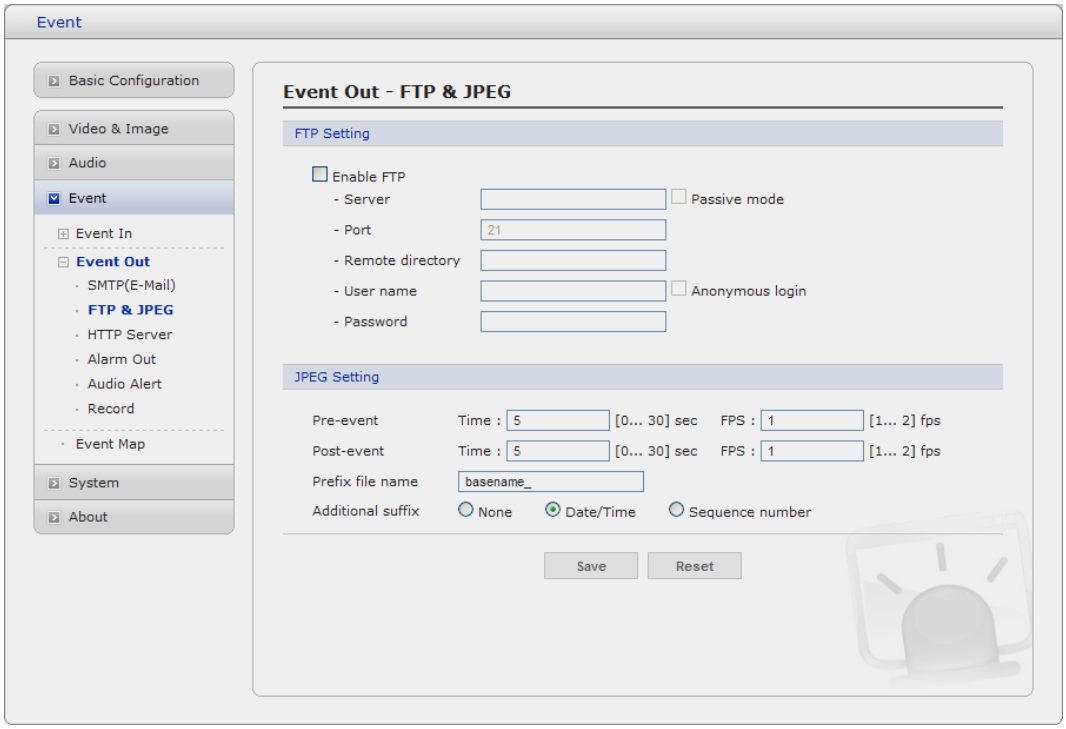
- **Login Method:** Set the Weakest method allowed to the highest/safest method supported by the mail server. The most secure method is listed in the drop-down list: Login / Plain

- **SMTP (E-Mail) Receiver**
  - **Receiver:** Enter an email address. You can also register the e-mail address of up to 8 recipients.

- **SMTP (E-Mail) Test**
  - **Receiver:** Enter an email address and click the Test button to test that the mail servers are functioning and that the email address is valid.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ FTP & JPEG



When the Network Camera detects an event, it can record and save images to an FTP server. Images can be sent as e-mail attachments. Check the box to enable the service.

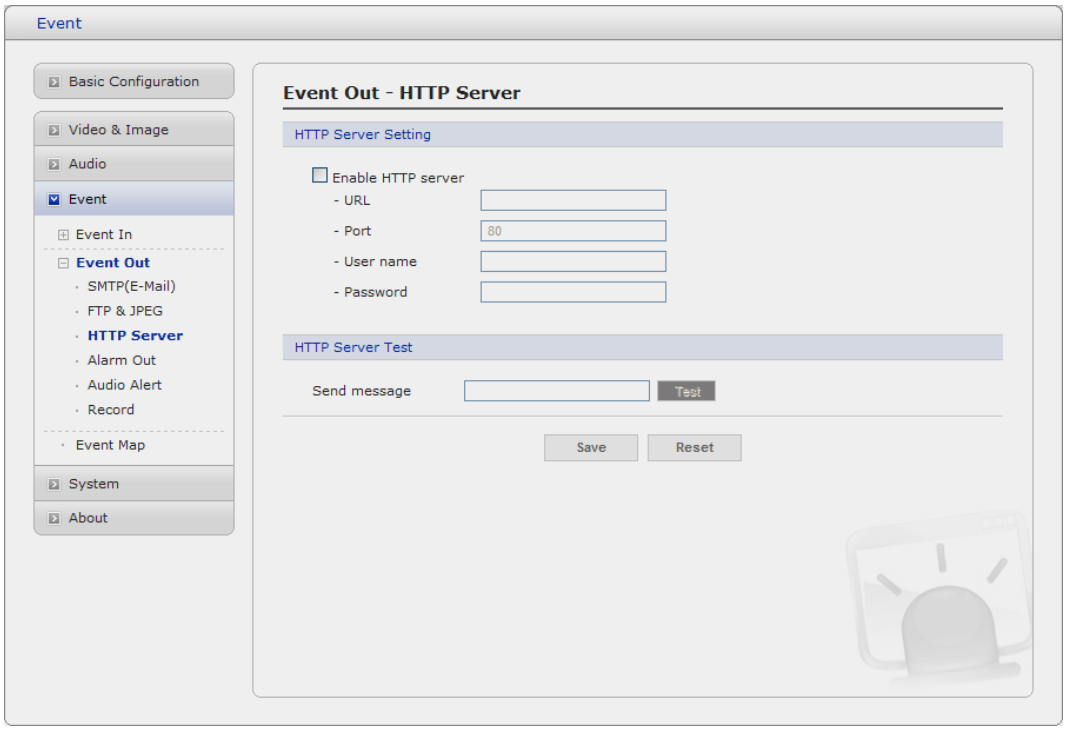
- **FTP Setting**
  - **Serve**r: Enter the server's IP address or host name. Note that a DNS server must be specified in the TCP/IP network settings if using a host name.
  - **Port:** Enter the port number used by the FTP server. The default is 21.
  - **Use passive mode:** Under normal circumstances the Network Camera simply requests the target FTP server to open the data connection. Checking this box issues a PASV command to the FTP server and establishes a passive FTP connection, whereby the Network Camera

actively initiates both the FTP control and data connections to the target server. This is normally desirable if there is a firewall between the camera and the target FTP server.

- **Remote directory:** Specify the path to the directory where the uploaded images will be stored. If this directory does not already exist on the FTP server, there will be an error message when uploading.
- **User name/Password:** Provide your log-in information.

- **JPEG Setting**
  - **Pre-event:** A pre-event buffer contains images from the time immediately preceding the event trigger. These are stored internally in the server. This buffer can be very useful when checking to see what happened to cause the event trigger.
    Check the box to enable the pre-trigger buffer, enter the desired total length in seconds, minutes or hours, and specify the required image frequency.
  - **Post-event:** This function is the counterpart to the pre-trigger buffer described above and contains images from the time immediately after the trigger. Configure as for pre-event.
  - **Prefix file name:** This name will be used for all the image files saved. If suffixes are also used, the file name will take the form <prefix>.<suffix>.<extension>.
  - **Additional suffix:** Add either a date/time suffix or a sequence number - with or without a maximum value.

▼ HTTP Server

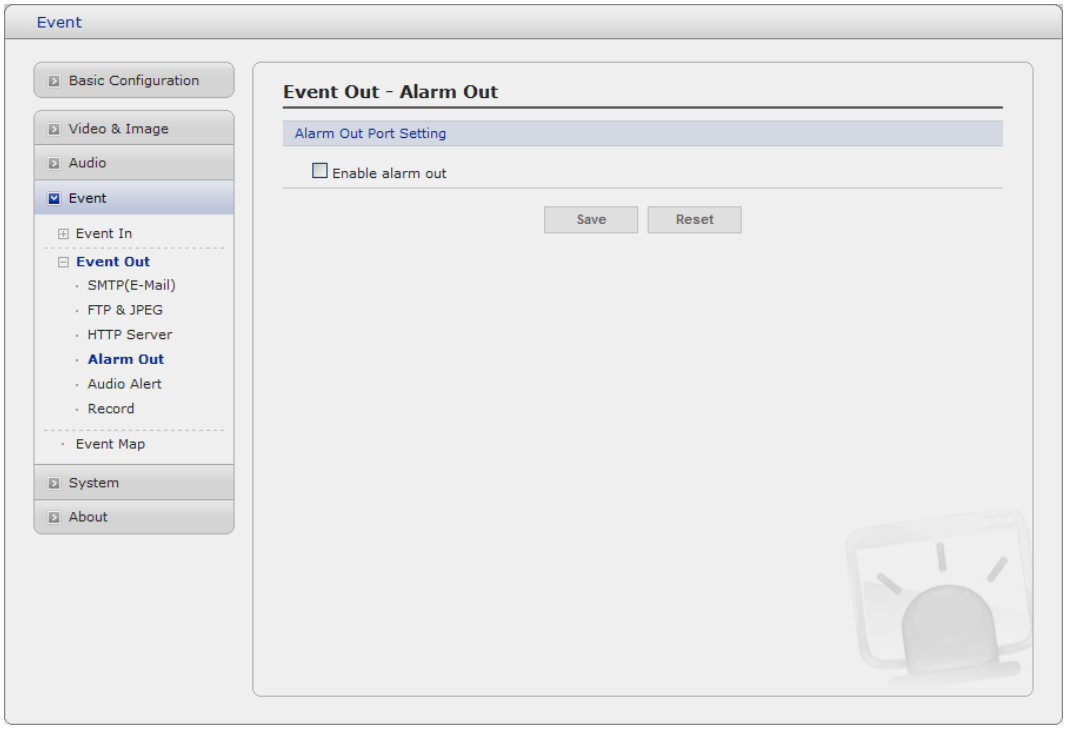


When the Network Camera detects an event, the HTTP Server is used to receive uploaded image files and/or notification messages. Check the box to enable the service.

- **HTTP Server Setting**
  - **Name:** The name of the HTTP event server; use a descriptive name.
  - **URL:** The network address to the server and the script that will handle the request. For example: http://192.168.12.244/cgi-bin/upload.cgi
  - **User name/Password:** Provide your log-in information.
- **HTTP Server Test**
  When the setup is complete, the connection can be tested by clicking the Test button.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Alarm Out

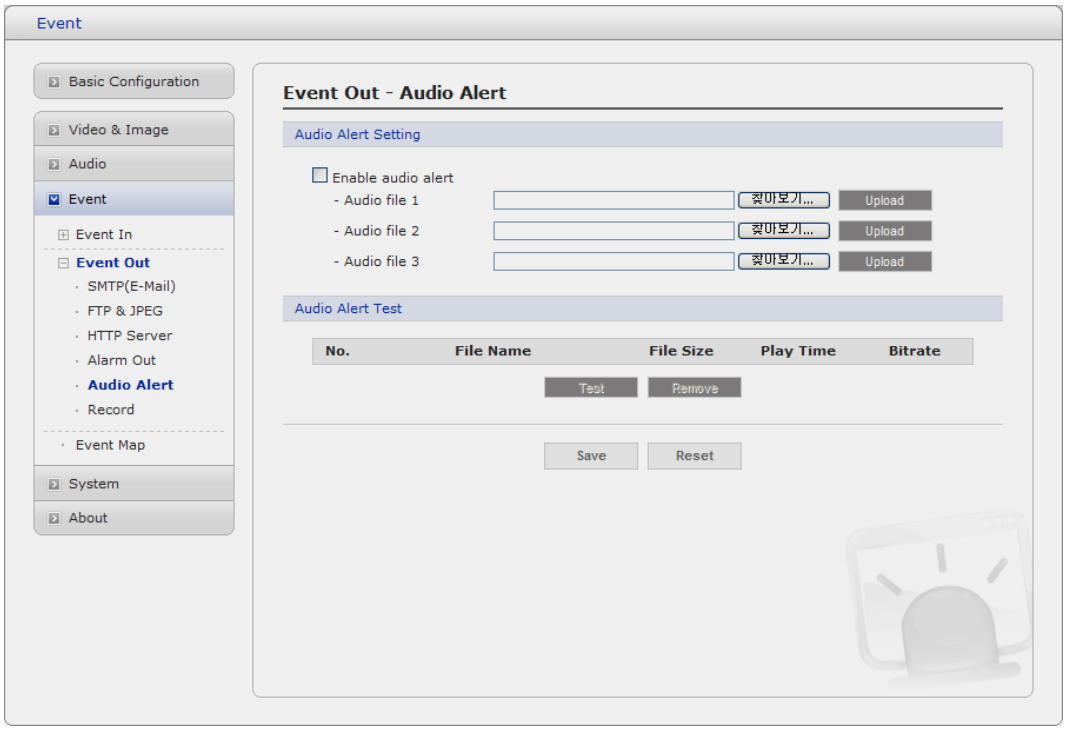


When the network camera detects an event, it can control external equipment connected to its alarm output port. Check the box to enable.

- When you select **"Enable alarm out"**, the output will be activated for as long as the event is active.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Audio Alert



When the Network Camera detects an event, it can output a predefined audio data to external speaker. Check the box to enable the service.

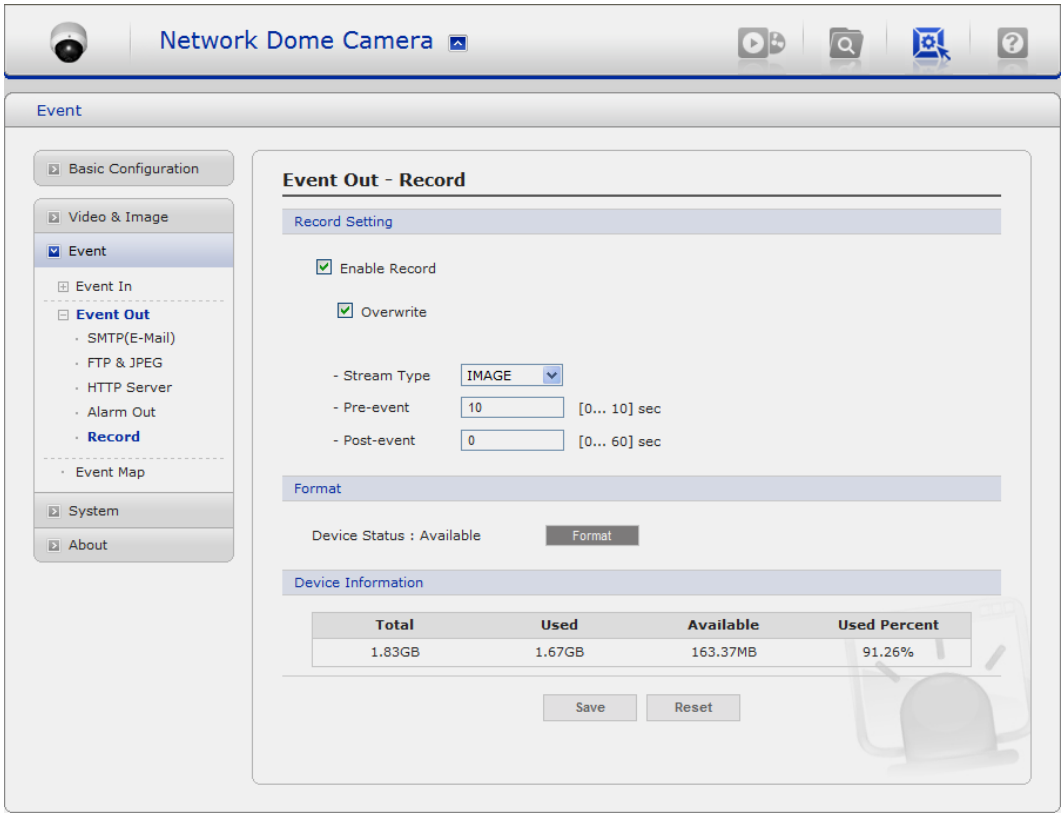
- **Audio Alert Setting**
  To use the audio alert with the Network camera, an audio data file made by user must be uploaded from your PC. Provide the path to the file directly, or use the Browse button to locate it. Then click the Upload button.

- **Audio Alert Test**
  When the setup is complete, the audio output can be tested by clicking the Test button.
  To remove an audio file, select index and click the Remove button.

Note: For a proper operation of Audio Alert, you must enable “Full duplex” in Audio setting page.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ **Record**



When the Network Camera detects an event, it can record the video stream in the Micro SD Memory. Check the box to enable the service.

- **Record Setting**
  - **Overwrite:** Click checkbox to overwrite the SD card.
  - **Stream Type:** You can select VIDEO or IMAGE.
  * VIDEO: H.264 or MPEG-4 data
  * IMAGE: MJPEG data
  - **Pre-event:** Enter pre-event time value for SD pre-recording.
  - **Post-event:** Enter post-event time value for SD post-recording.

- **Format**

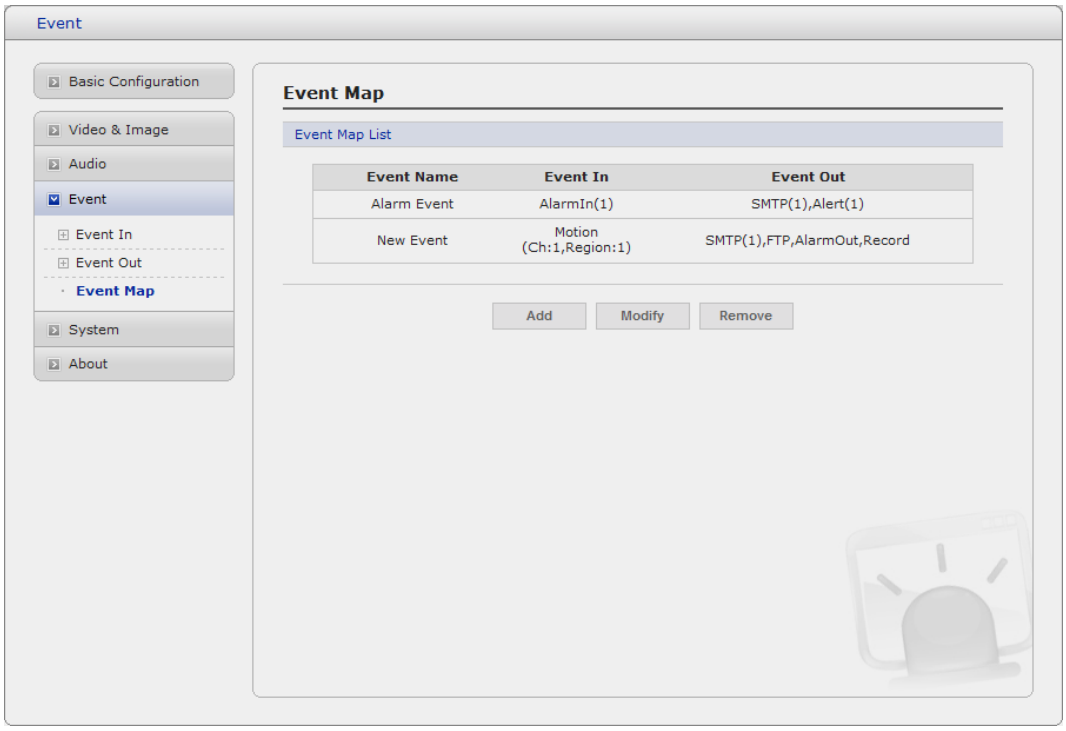
  Click the Format button to format SD card.

- **Device Information**

  Shows current SD card information.

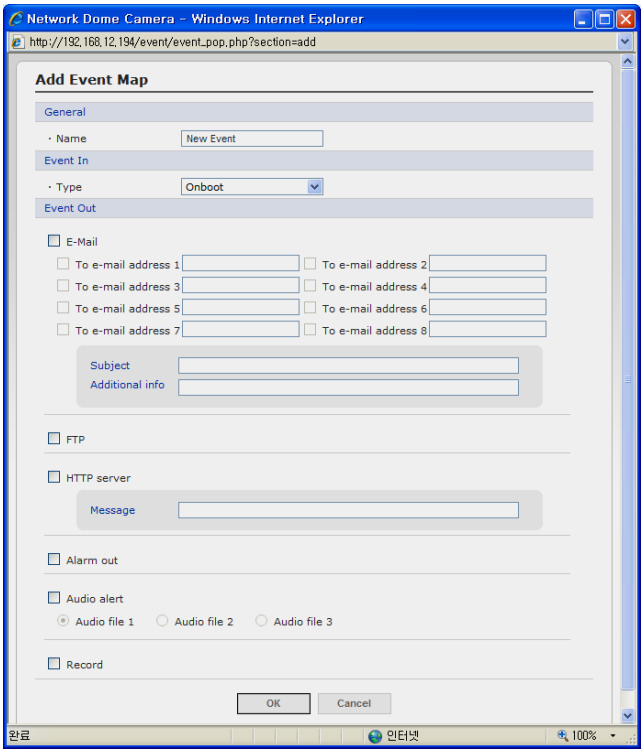
When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

3) Event Map



The event map allows you to change the settings and establish a schedule for each event trigger from the Network Camera. You can register the event map up to max. 15.

Click Add button to make a new event map; a popup window displays as below. To change an existing event, select that event and click the Modify button; this same window will display and the information can be changed as required. Selecting an event and clicking Remove deletes the event.



- **General**
  Enter the name for a new event map.

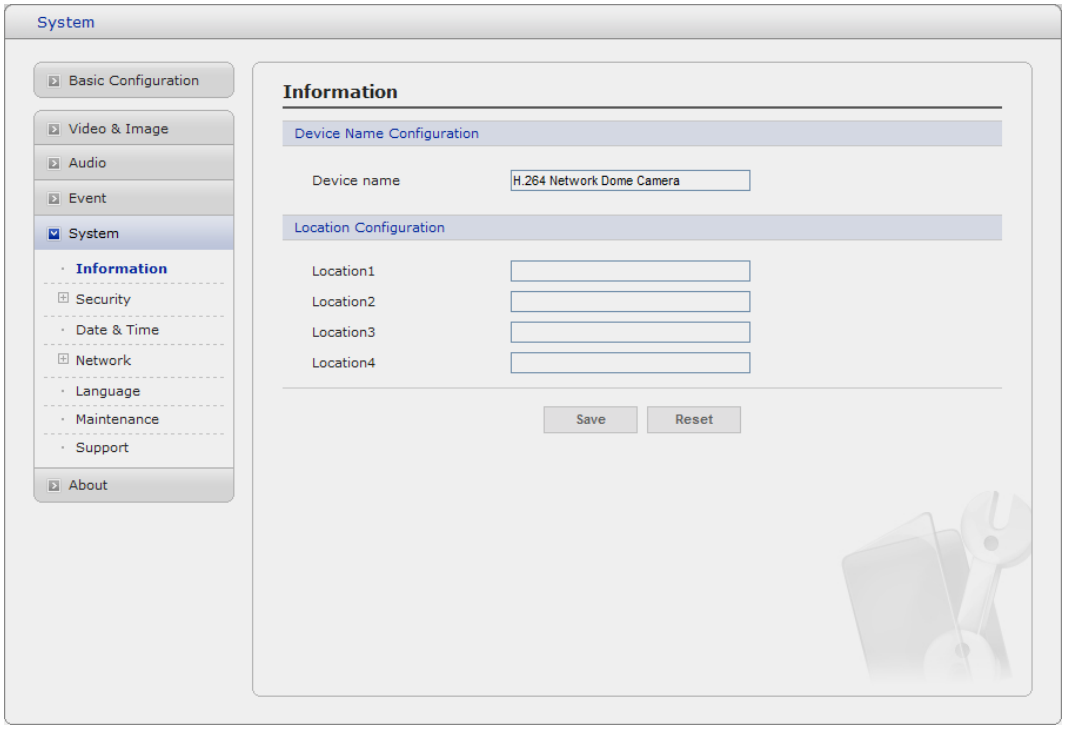
- **Event In**
  Select an event type in the drop down list.

- **Event Out**
  - **E-mail:** Select email addresses to send via email that an event has occurred.
  - **FTP:** Select checkbox beside FTP to record and save images to an FTP server when an event has occurred.
  - **HTTP Server:** Send notification messages to an HTTP server that listens for these. The destination server must first be configured on the Event In page. Enter a message you want to send.
  - **Record:** Select Record checkbox to record the video stream when an event has occurred. The Record option must first be configured on the Event Out page.

3.5.5 System

1) Information

You can enter the system information. This page is very useful when you need to refer to device information after installation.



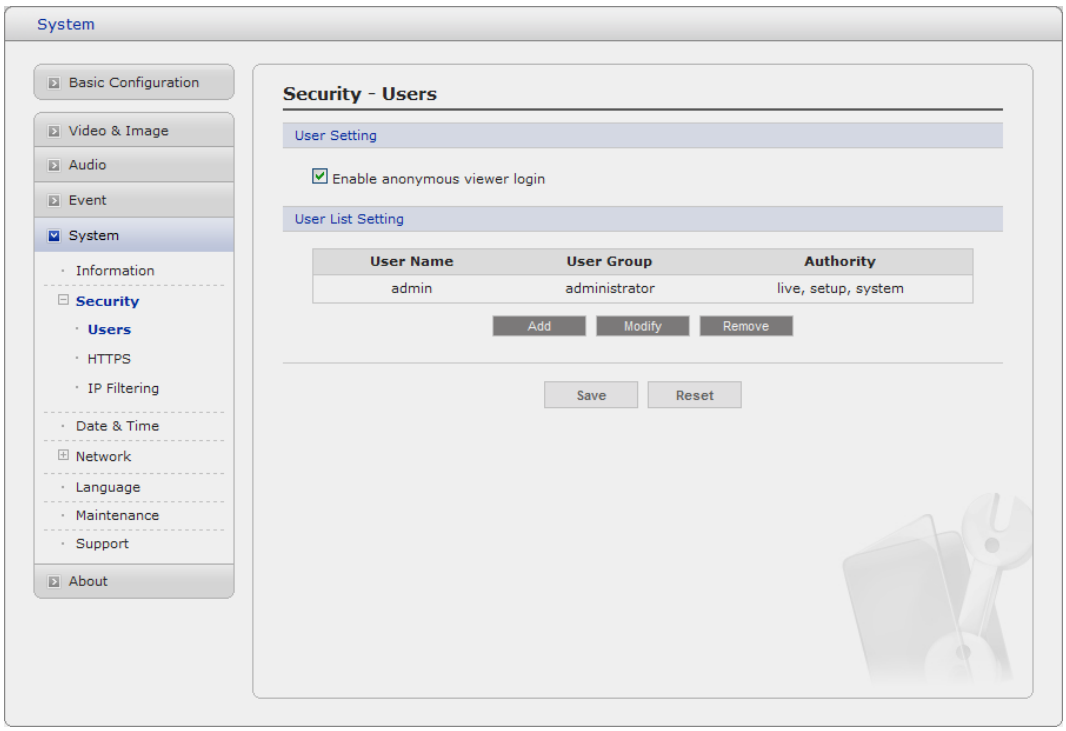
- **Device Name Configuration**
  Enter the device name.

- **Location Configuration**
  Enter the location information. You can enter up to four.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

2) Security

▼ Users

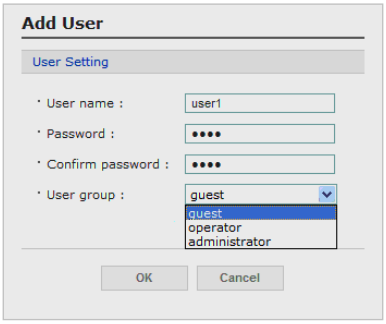


User access control is enabled by default when the administrator sets the root password on first access. New users are authorized with user names and passwords, or the administrator can choose to allow anonymous viewer login to the Live View page, as described below:

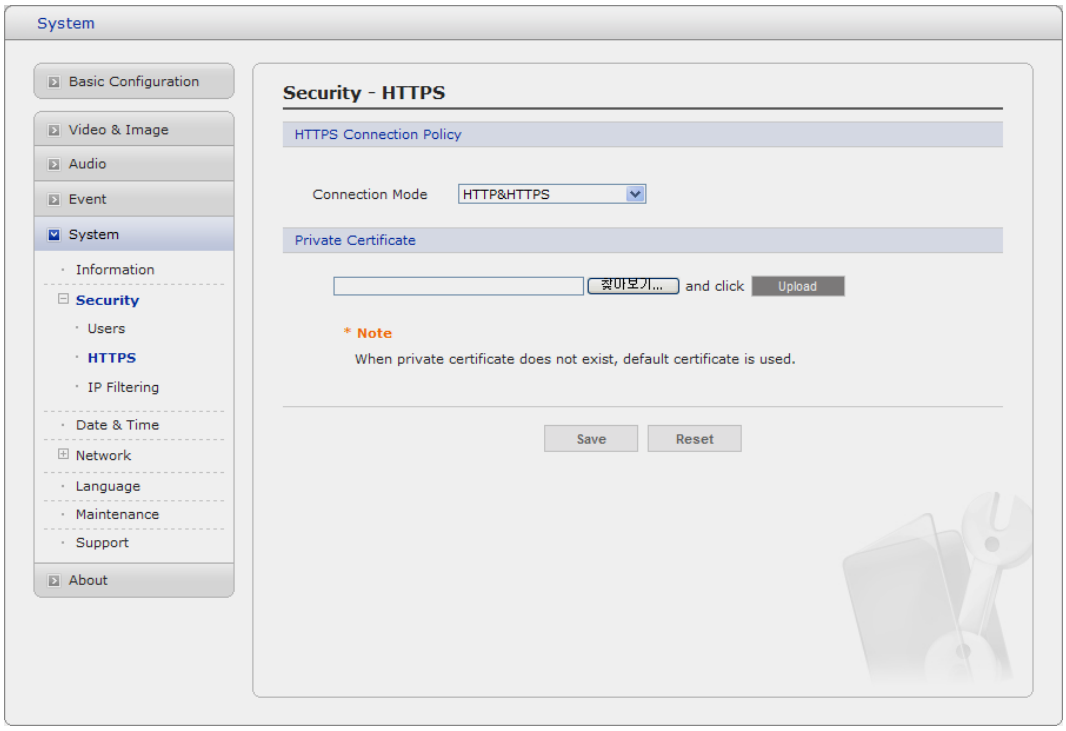
- **User Setting**
  Check the box to enable anonymous viewer login to the Network Camera without a user account. When using the user account, users have to log-in at every access.

- **User List Setting**

This section shows a list of registered user accounts. Press the Add button; the pop-up window displays as below. Enter a user name and password to be added and select the user group from the drop-down list; click OK to register the user or Cancel to negate the user. User information can also be modified by selecting the user from the list and clicking the Modify button; this same screen will display. Change any information as needed. Selecting a user and clicking Remove deletes the user.



▼ HTTPS



For greater security, the Network Camera can be configured to use HTTPS [Hypertext Transfer Protocol over SSL (Secure Socket Layer)]; all communication that would otherwise go via HTTP will instead go via an encrypted HTTPS connection.

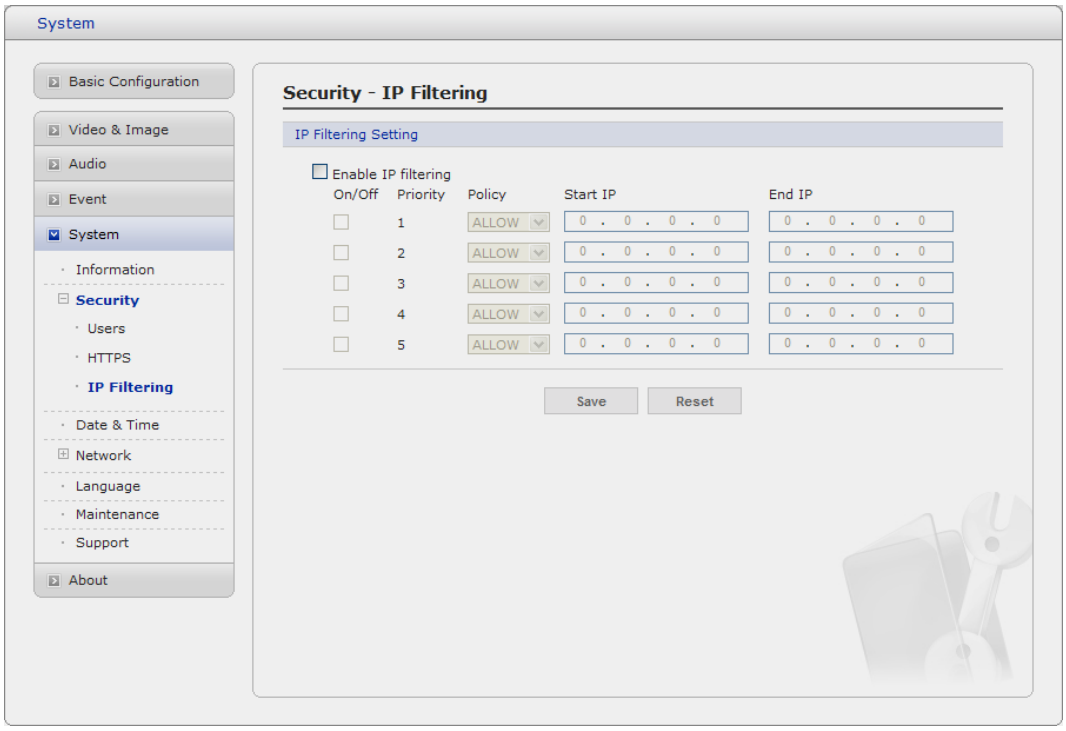
- **HTTPS Connection Policy**
  Choose the form of connection mode you wish to use from the drop-down list for the administrator, Operator and Viewer to enable HTTPS connection (set to HTTP by default).
  - **HTTP**
  - **HTTPS**
  - **HTTP & HTTPS**

- **Upload Certificate**
  To use HTTPS for communication with the Network Camera, an official certificate issued by a CA (Certificate Authority) must be uploaded from your PC. Provide the path to the certificate directly, or use the **Browse** button to locate it. Then click the **Upload** button.

Refer to the home page of your preferred CA for information on where to send the request.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ IP Filtering



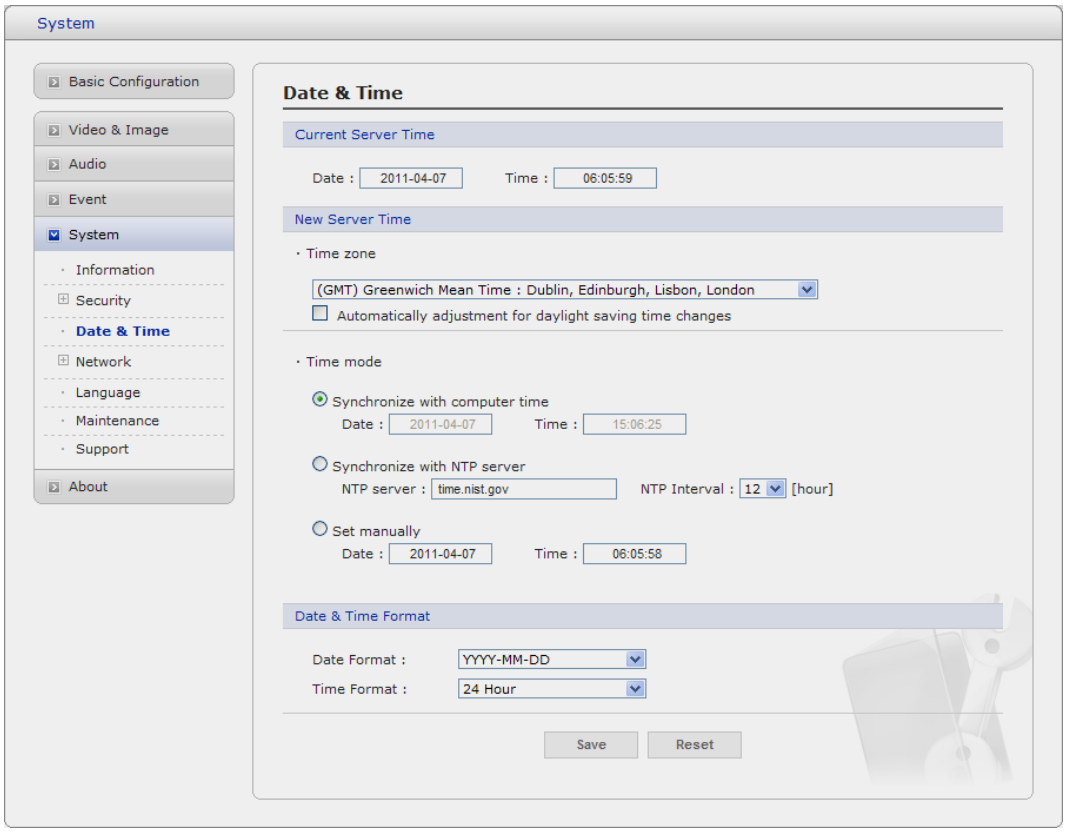
Checking the **Enable IP address filtering** box enables the IP address filtering function. Up to 256 IP address entries may be specified (a single entry can contain multiple IP addresses). Click the **Add** button to add new filtered addresses.

When the IP address filter is enabled, addresses added to the list are set as Allowed ***or*** Denied addresses. All other IP addresses not in this list will then be allowed or denied access accordingly, that is, if the addresses in the list are allowed, then all others are denied access, and vice versa.

Note that users from IP addresses that will be allowed must also be registered with the appropriate access rights (Guest, Operator or Administrator). This is done from Setup> System>Security>Users.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

3) Date & Time



- **Current Server Time**
  It displays the current date and time (24h clock). The time can be displayed in 12h clock format in the overlay.

- **New Server Time**
  Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select “Automatically adjustment for daylight saving time changes”.

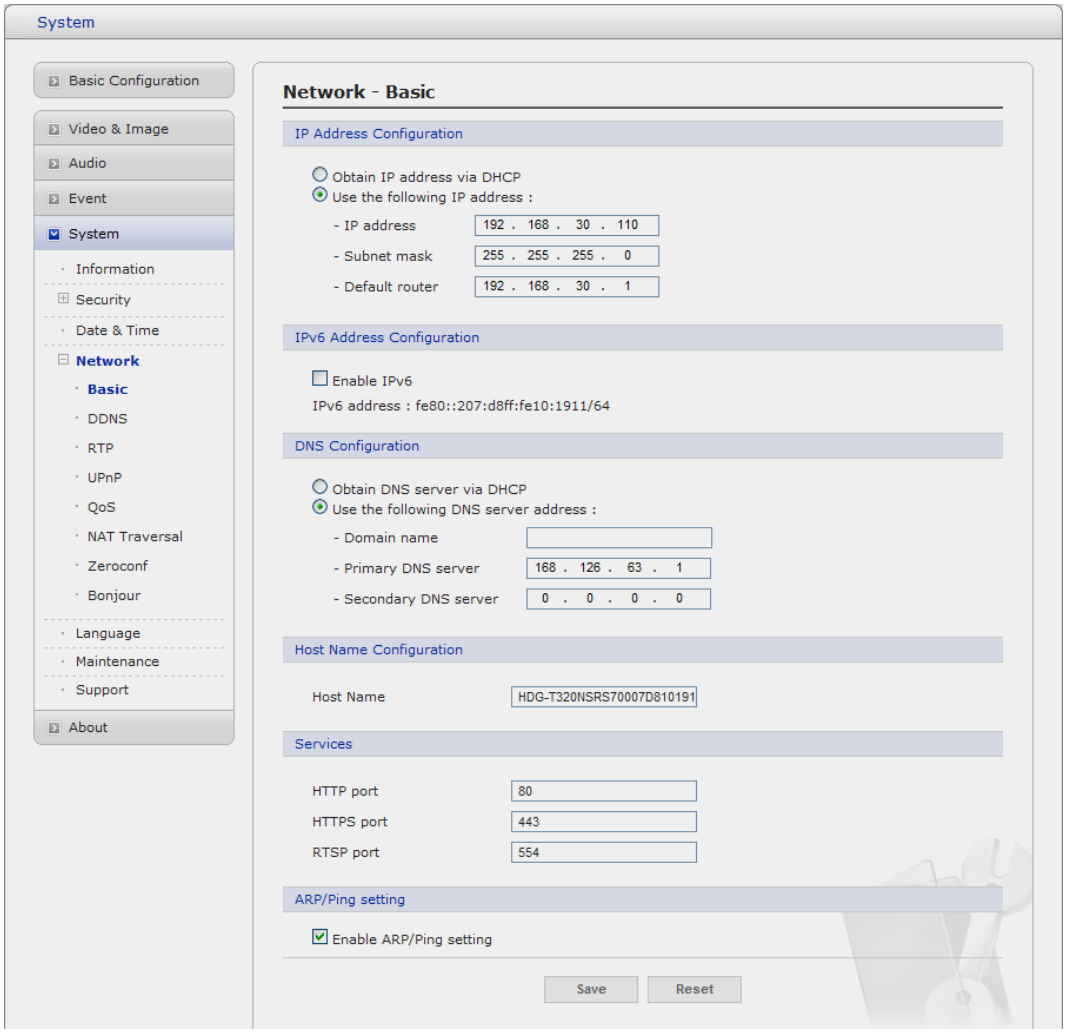
  From the Time Mode section, select the preferred method to use for setting the time:
  - **Synchronize with computer time:** sets the time from the clock on your computer.
  - **Synchronize with NTP Server:** the video encoder will obtain the time from an NTP server every 60 minutes.
  - **Set manually:** this option allows you to manually set the time and date.

- **Date & Time Format**
  Specify the formats for the date and time (12h or 24h) displayed in the video streams.
  Select Date & Time format from the drop-down list.
  - **Date Format:** Specify the date format. YYYY: Year, MM: Month, DD: Day
  - **Time Format:** Specify the date format. 24 Hours or 12 Hours

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

Note: Note that if using a host name for the NTP server, a DNS server must be configured under TCP/IP settings.

4) Network



Setting regarding the network can be executed. Settings for IP, DNS, Host Name, Port, and ARP/Ping can be established, along with setting for DDNS, uPnP, QoS, Zeroconfig, and Bonjour.

▼ **Basic**

- **IP Address Configuration:**
  - **Obtain IP address via DHCP:** Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.
  - **Use the following IP address:** To use a static IP address for the Network Camera, check the radio button and then make the following settings:
  * **IP address:** Specify a unique IP address for your Network Camera.
  * **Subnet mask:** Specify the mask for the subnet the Network Camera is located on.
  * **Default router:** Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

- **IPv6 Address Configuration**
  Check this box to enable IPv6. Other settings for IPv6 are configured in the network router.

- **DNS Configuration**
  DNS (Domain Name Service) provides the translation of host names to IP addresses on your network.
  - **Obtain DNS Server via DHCP:** Automatically use the DNS server settings provided by the DHCP server. Click the View button to see the current settings.
  - Use the following DNS server address to enter the desired DNS server by specifying the following:
  * **Domain name:** Enter the domain(s) to search for the host name used by the Network Camera. Multiple domains can be separated by semicolons (;). The host name is always the first part of a Fully Qualified Domain Name, for example, myserver is the host name in the Fully Qualified Domain Name myserver.mycompany.com where mycompany.com is the Domain name.
  * **DNS servers:** Enter the IP addresses of the primary and secondary DNS servers.

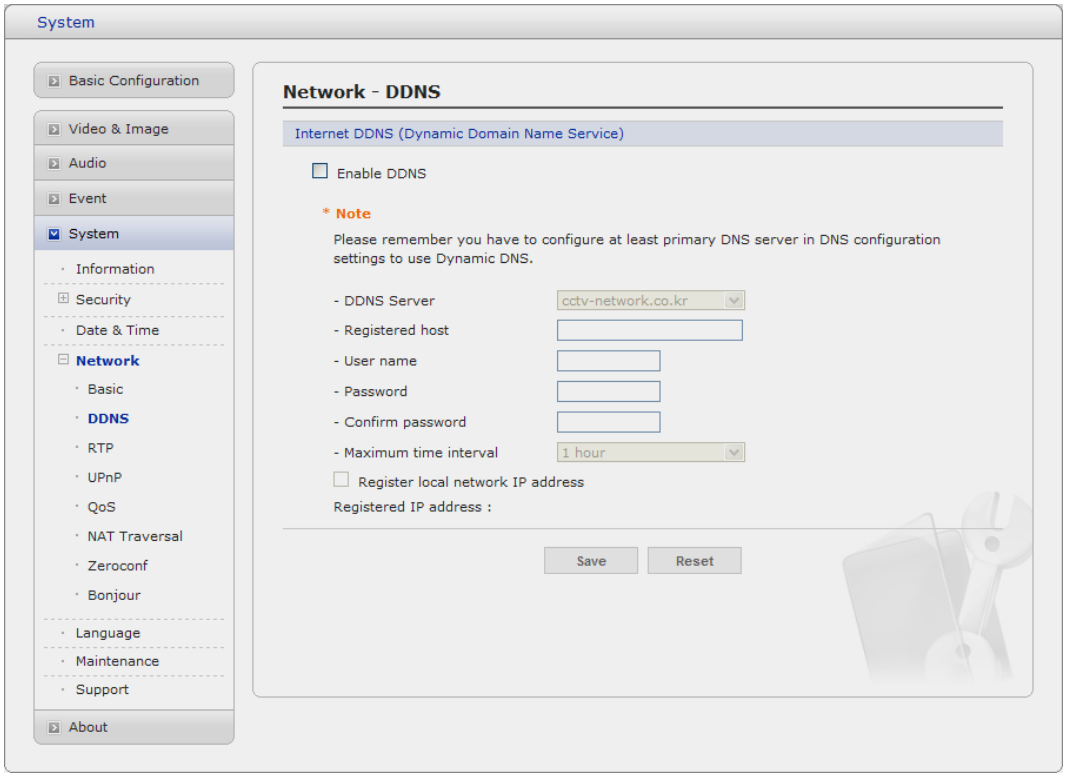
- **Host Name Configuration**
  - **Host Name** – Enter the host name to be used as device information in the client software or SmartManager.

- **Services**
  - **HTTP port:** Enter a port to receive a service through the HTTP. Default Port Number is '80'.
  - **RTSP port:** Enter a port to receive a service through the RTSP. Default Port Number is '7070'.

- **ARP/Ping Setting**
  - Enable ARP/Ping setting of IP address - The IP address can be set using the ARP/Ping method, which associates the unit's MAC address with an IP address. Check this box to enable the service. Leave disabled to prevent unintentional resetting of the IP address.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ DDNS

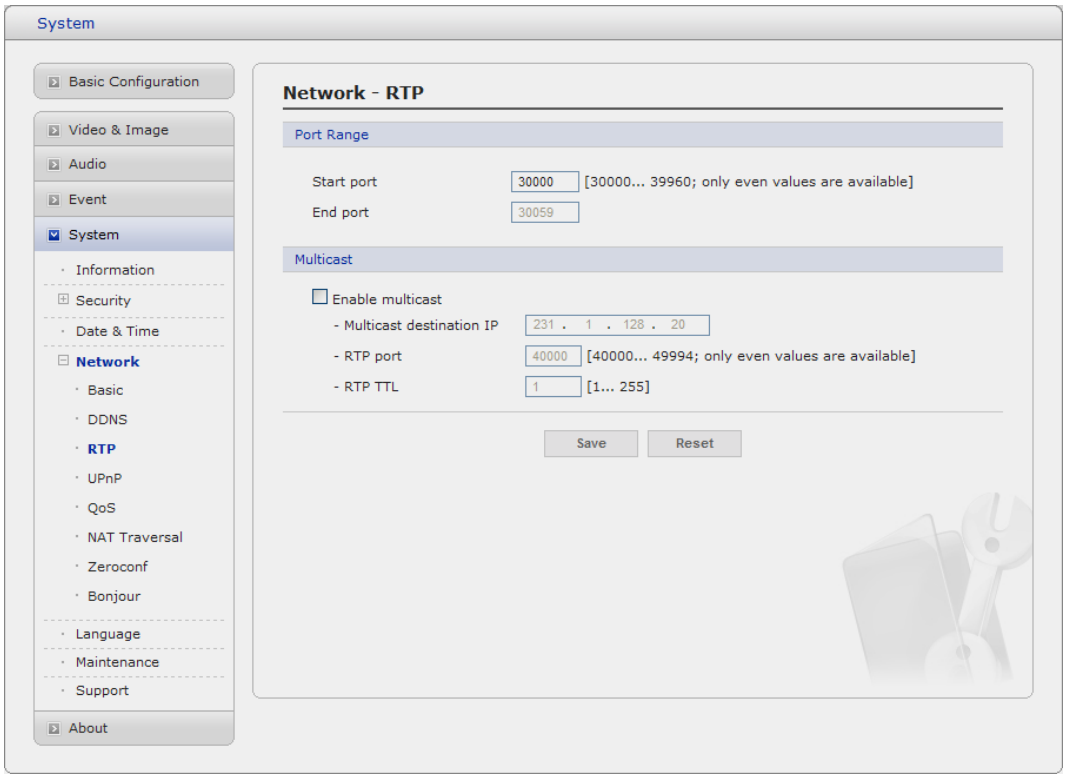


- **Internet DDNS (Dynamic Domain Name Service)**
  When using the high-speed Internet with the telephone or cable network, users can operate the Network Camera even on the floating IP environment in which IPs are changed at every access. Users should receive an account and password by visiting a DDNS service like http://www.dyndns.com/.

  - **Enable DDNS:** Check to get DDNS service to be available.
  * **DDNS Server:** Select the DDNS server.
  * **Registered host:** Enter an address of the DDNS server.
  * **Username:** Enter an ID to access to the DDNS server.
  * **Password:** Enter a password to be used for accessing the DDNS server.
  * **Confirm:** Enter a password again to confirm it.
  * **Maximum time interval:** Set a time interval to synchronize with the DDNS server. Select from the interval drop-down list.
  * **Register local network IP address:** Register a Network Video Server IP address to the DDNS server.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ RTP



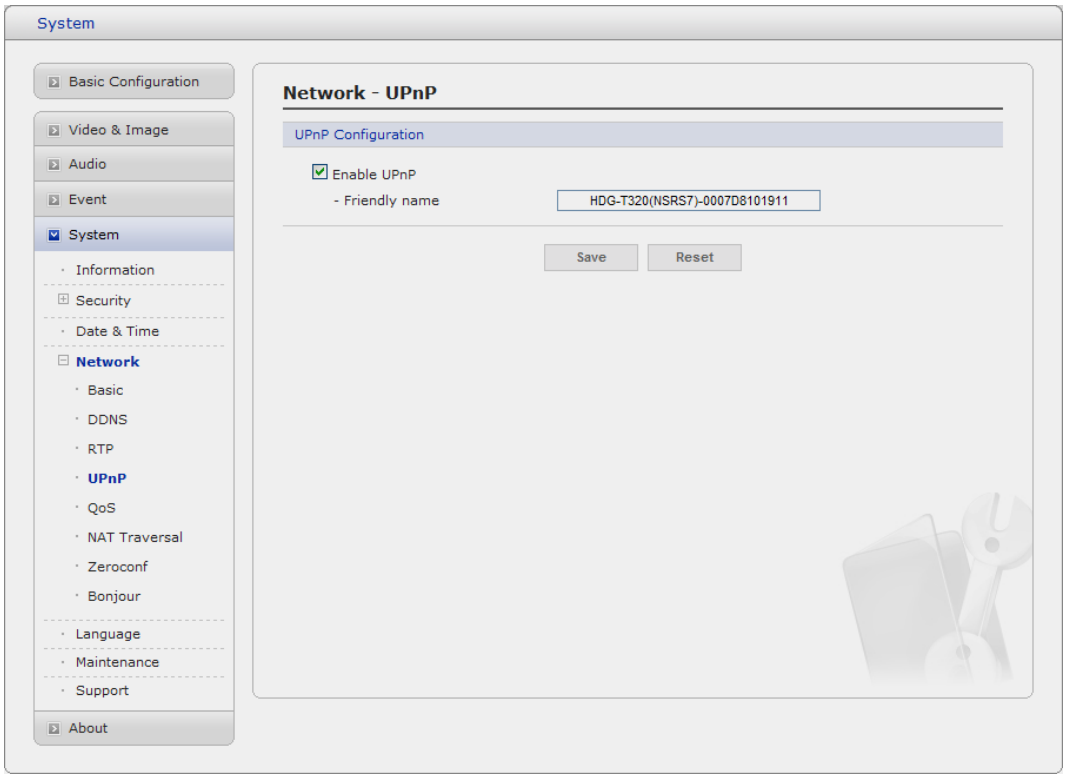
Create a setting for sending and receiving an audio or video on a real-time basis. These settings are the IP address, port number, and Time-To-Live value to use for the media stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams. For more information, see the online help.

- **Port Range**
  - **Start port:** Enter a value between 1024 and 65532.

- **Multicast**
  This function is for sending Video and Audio to Multicast group.
  - **Enable multicast:** Check the box to enable multicast operation.
  - **Multicast destination IP:** Enter an IP between 224.0.0.0 and 239.255.255.255. Although it is empty, an IP will be entered automatically.
  - **RTP port:** Enter a value between 1024 and 65532.
  - **RTP TTL:** Enter a value between 1 and 255. If a network status is smooth, enter a lower value. On the other hand, if a network status is poor, enter a higher value. When there are many Network Cameras or users, a higher value may cause a heavy load to the network. For a detailed setting, please consult with a network manager.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ UPnP



The Network Camera includes support for UPnP™. UPnP is enabled by default, so the Network Camera is automatically detected by operating systems and clients that support this protocol. Enter a name in the Friendly field.

Note: UPnP must be installed on your workstation if running Windows® XP. To do this, open the Control Panel from the Start Menu and select Add/Remove Programs. Select Add/Remove Windows Components and open the Networking Services section. Click Details and then select UPnP as the service to add.

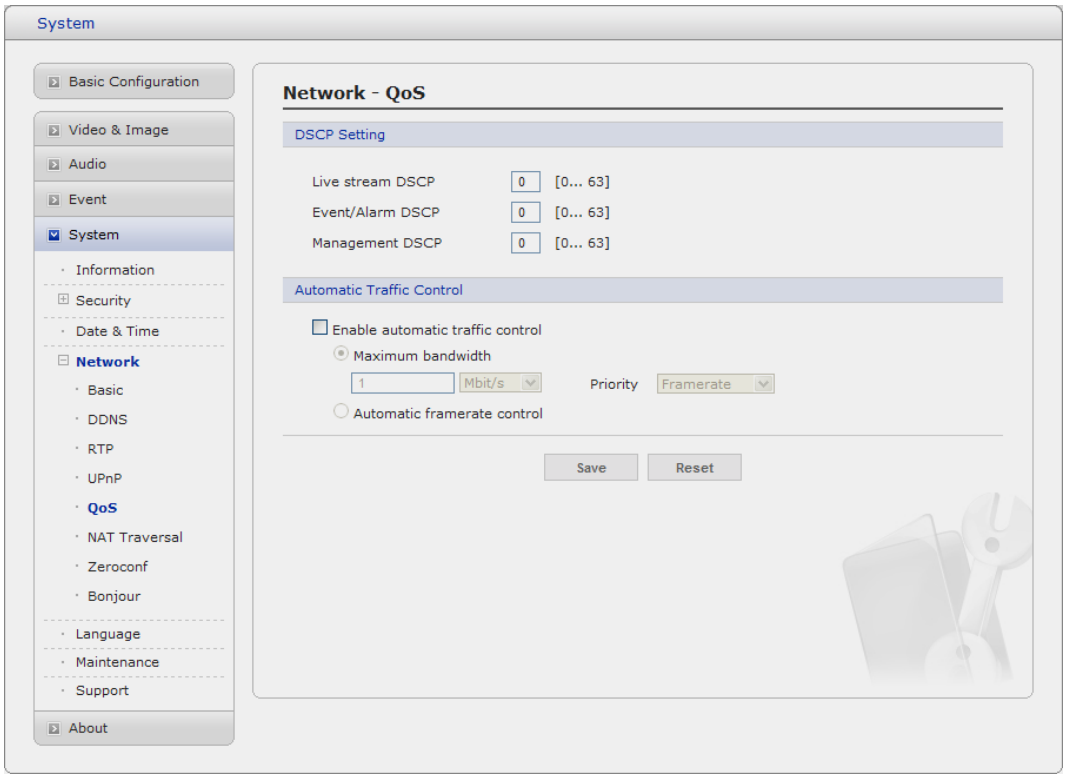
When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ QoS

Quality of Service (QoS) provides the means to guarantee a certain level of a specified resource to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses.

The main benefits of a QoS-aware network are:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- Greater reliability in the network, due to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.



- **DSCP Settings**
  For each type of network traffic supported by your network video product, enter a DSCP (Differentiated Services Code Point) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch which type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal.

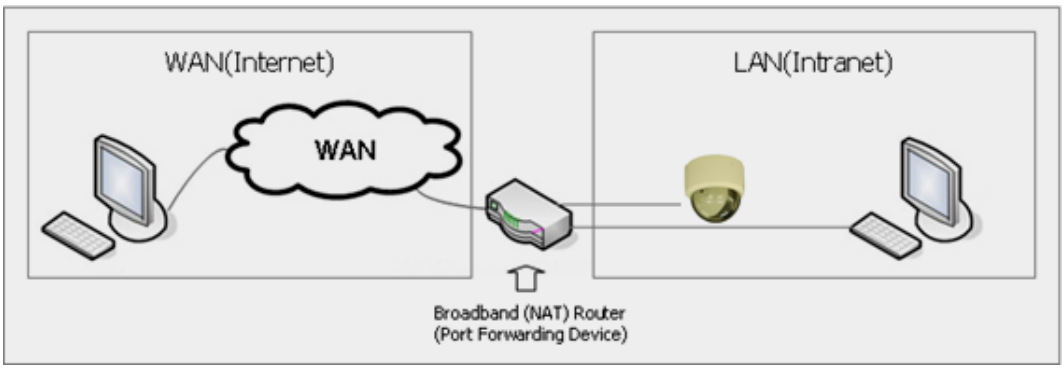
  The following types of traffic are marked:
  - **Live Stream DSCP:**
  - **Event/Alarm DSCP:**
  - **Management DSCP:**

- **Auto Traffic Control**
  Set a limitation on user network resources by designating the maximum bandwidth.
  - Maximum bandwidth - When sharing other network programs or equipment, it is possible to set a limitation on the maximum bandwidth in the unit of Mbit/s or kbit/s.
  - Auto frame rate - Selected if not influenced by a network-related program or equipment without a limitation on the network bandwidth.

▼ NAT Traversal

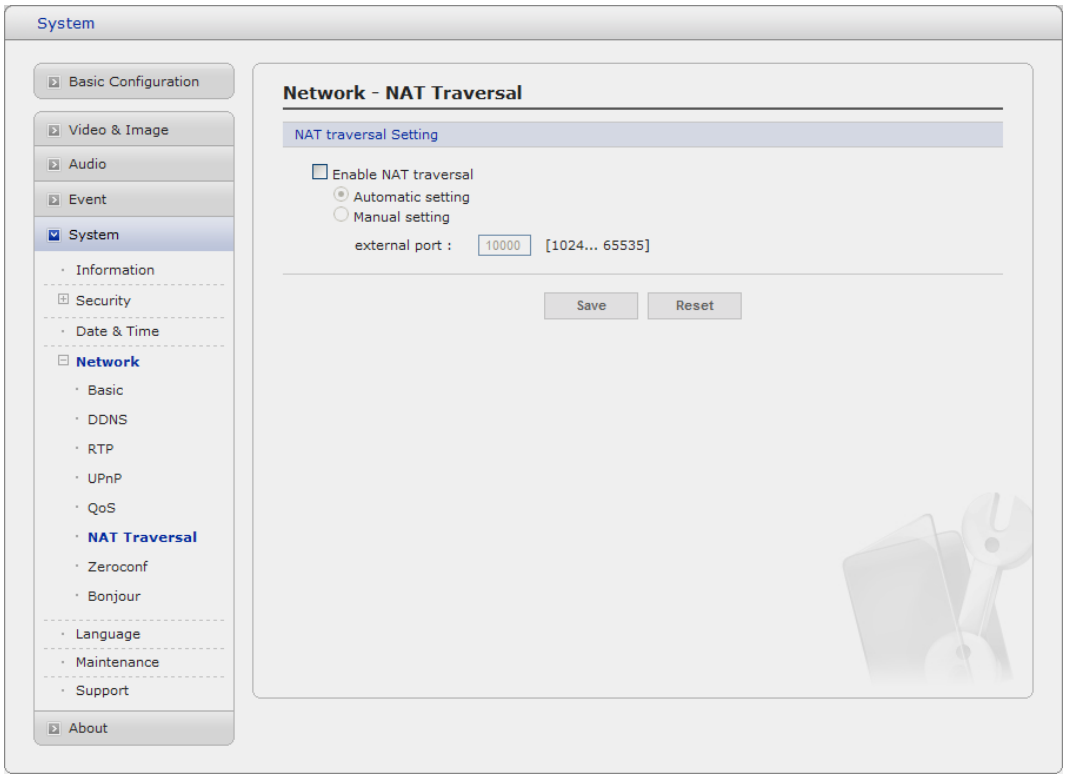
A broadband router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the “outside”, that is, the Internet. Security on the private network (LAN) is increased since most broadband routers are pre-configured to stop attempts to access the private network (LAN) from the public network/Internet.

Use **NAT traversal** when your network cameras are located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the network camera.



Notes:

- For NAT traversal to work, this must be supported by the broadband router.
- The broadband router has many different names:
  “NAT router”, “Network router“, Internet Gateway”, “Broadband sharing device” or “Home firewall” but the essential purpose of the device is the same.



- **NAT traversal Settings**
  - **Enabl**e - when enabled, the network transmitters attempt to configure port mapping in a NAT router on your network, using UPnP. Note that UPnP must be enabled in the Network Camera (see System>Network>UPnP).
  * **Automatic setting:** The Network Camera automatically searches for NAT routers on your network.
  * **Manual setting:** Select this option to manually select a NAT router and enter the external port number for the router in the field provided.

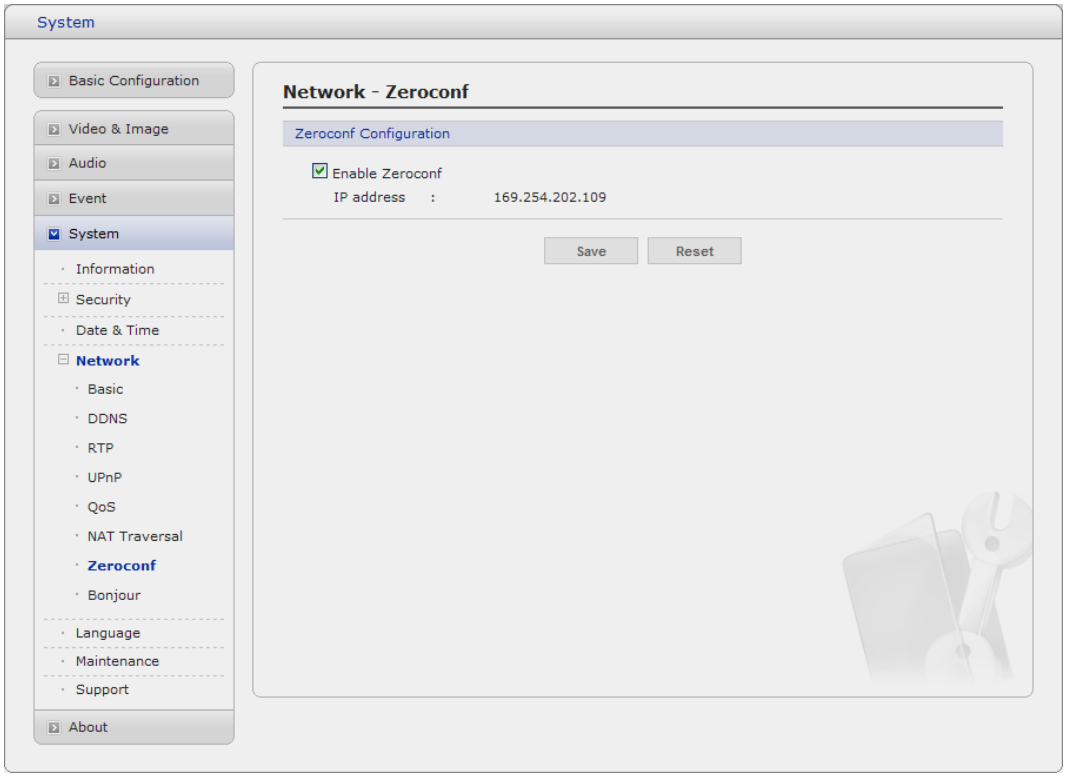
Notes:

- If you attempt to manually enter a port that is already in use, an alert message will be displayed.
- When the port is selected automatically it is displayed in this field. To change this, enter a new port number and click Save.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Zeroconfig

Zeroconfig allows the Network Camera to create and assign an IP address for network cameras and connect to a network automatically.



Zero configuration networking (zeroconf) is a set of techniques that automatically creates a usable Internet Protocol (IP) network without manual operator intervention or special configuration servers.

Zero configuration networking allows devices such as computers and printers to connect to a network automatically. Without zeroconf, a network administrator must set up services, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS), or configure each computer's network settings manually, which may be difficult and time-consuming.

Zeroconf is built on three core technologies:

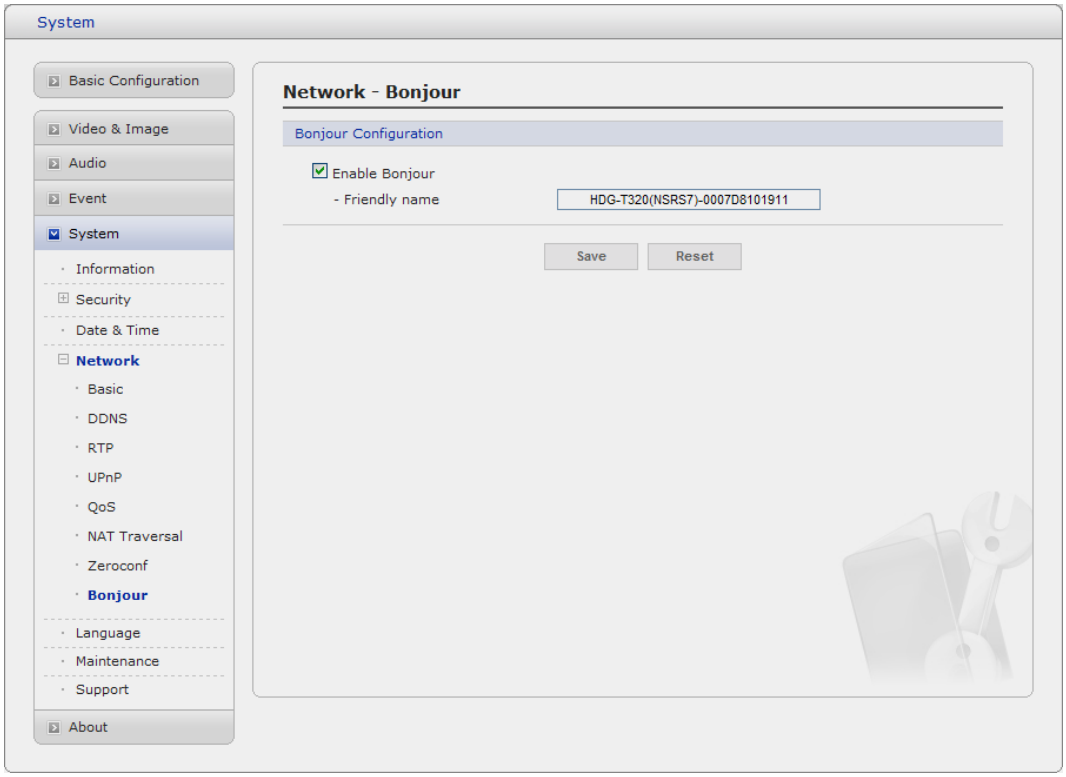
- Assignment of numeric network addresses for networked devices (link-local address auto configuration).
- Automatic resolution and distribution of computer hostnames (multicast DNS).
- Automatic location of network services, such as printing devices through DNS service discovery.

Click the checkbox to enable Zeroconfig.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Bonjour

The Network Camera includes support for Bonjour™. When enabled, the Network Camera is automatically detected by operating systems and clients that support this protocol.



Click the checkbox to enable Bonjour. Enter a name in the Friendly name field.

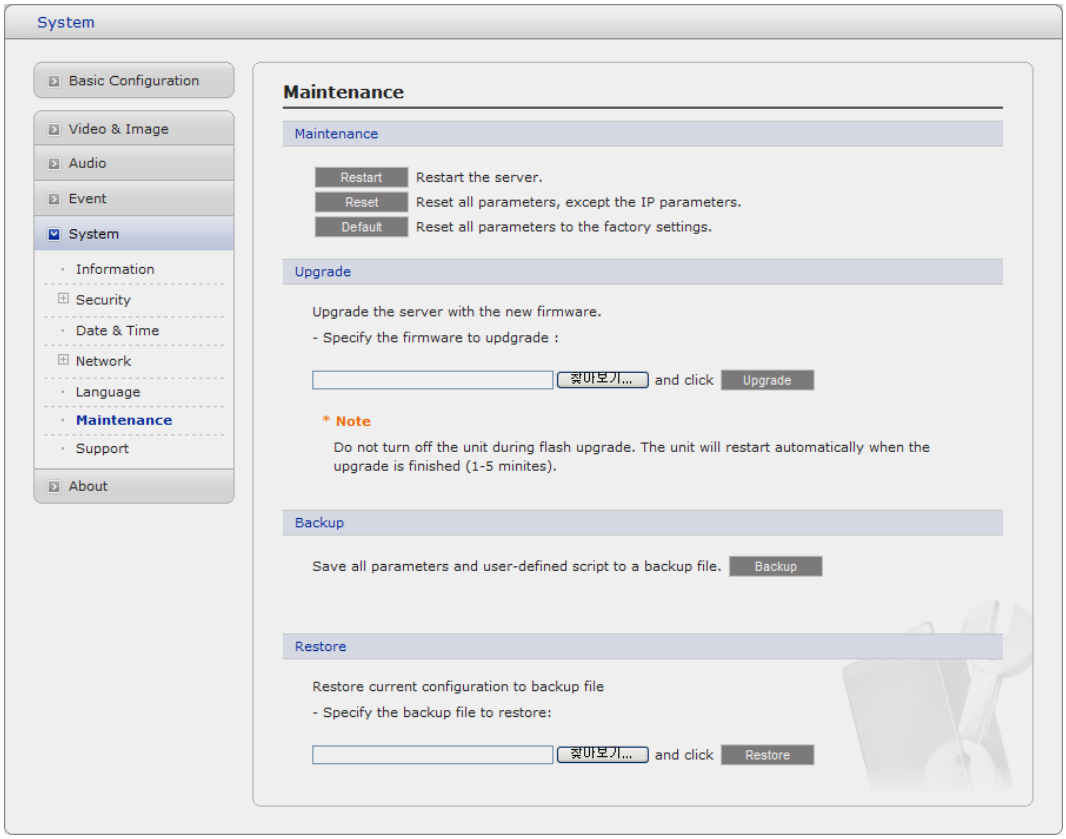
When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

Note: Bonjour - Also known as zero-configuration networking, Bonjour enables devices to automatically discover each other on a network, without having to enter IP addresses or configure DNS servers. Bonjour is a trademark of Apple Computer, Inc.

5) Language

Select a user language. The language choices are English, French, German, Spanish and Italian.

6) Maintenance



- **Maintenance Server**
  - **Restart:** The unit is restarted without changing any of the settings. Use this method if the unit is not behaving as expected.
  - **Reset:** The unit is restarted and most current settings are reset to factory default values. The settings that are not affected are:
    * the boot protocol (DHCP or static)
    * the static IP address
    * the default router
    * the subnet mask
    * the system time
  - **Default:** The default button should be used with caution. Pressing this will return all of the Network Camera's settings to the factory default values (including the IP address).

- **Upgrade**
  Upgrade the camera by importing an upgrade file and pressing the Upgrade button. During the upgrade, do not turn off the power to the Network Camera. After waiting at least five minutes, try to access the camera again.

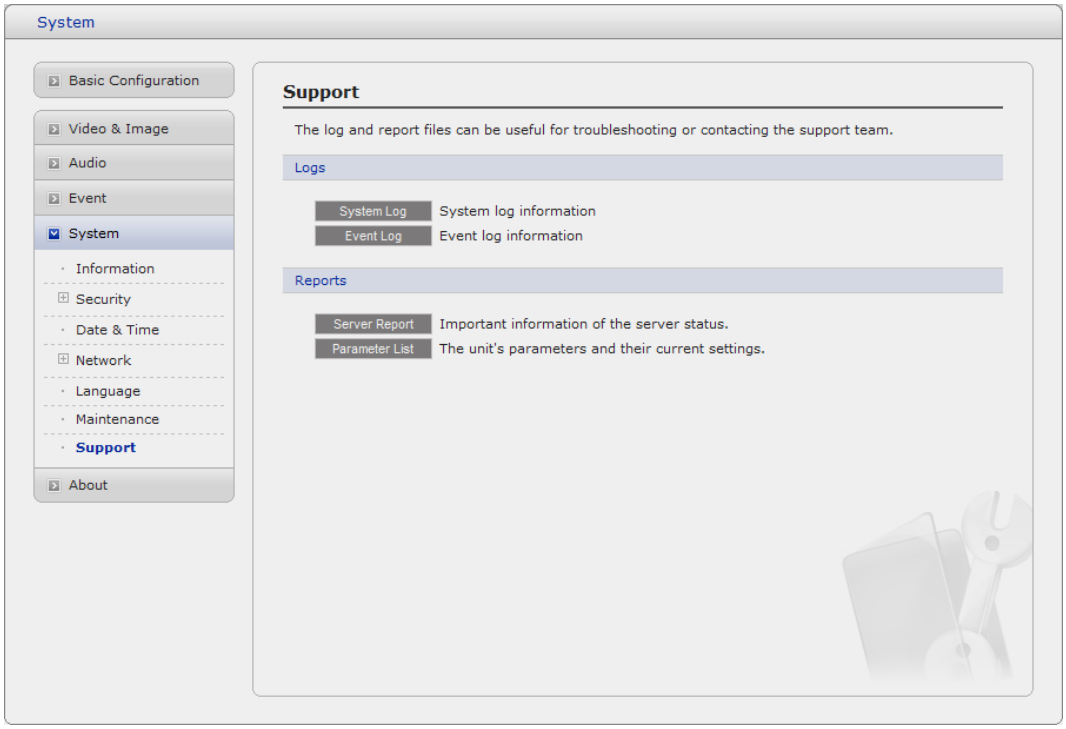
- **Backup**
  Click the **Backup** button to save setting values that users enter to the network camera to a user PC.

- **Restore**
  Click the **Restore** button to import and apply setting values saved to a user PC.

  Note: Backup and Restore can only be used on the same unit running the same firmware. This feature is not intended for multi-configurations or for firmware upgrades.

7) Support

The support page provides valuable information on troubleshooting and contact information, should you require technical assistance.

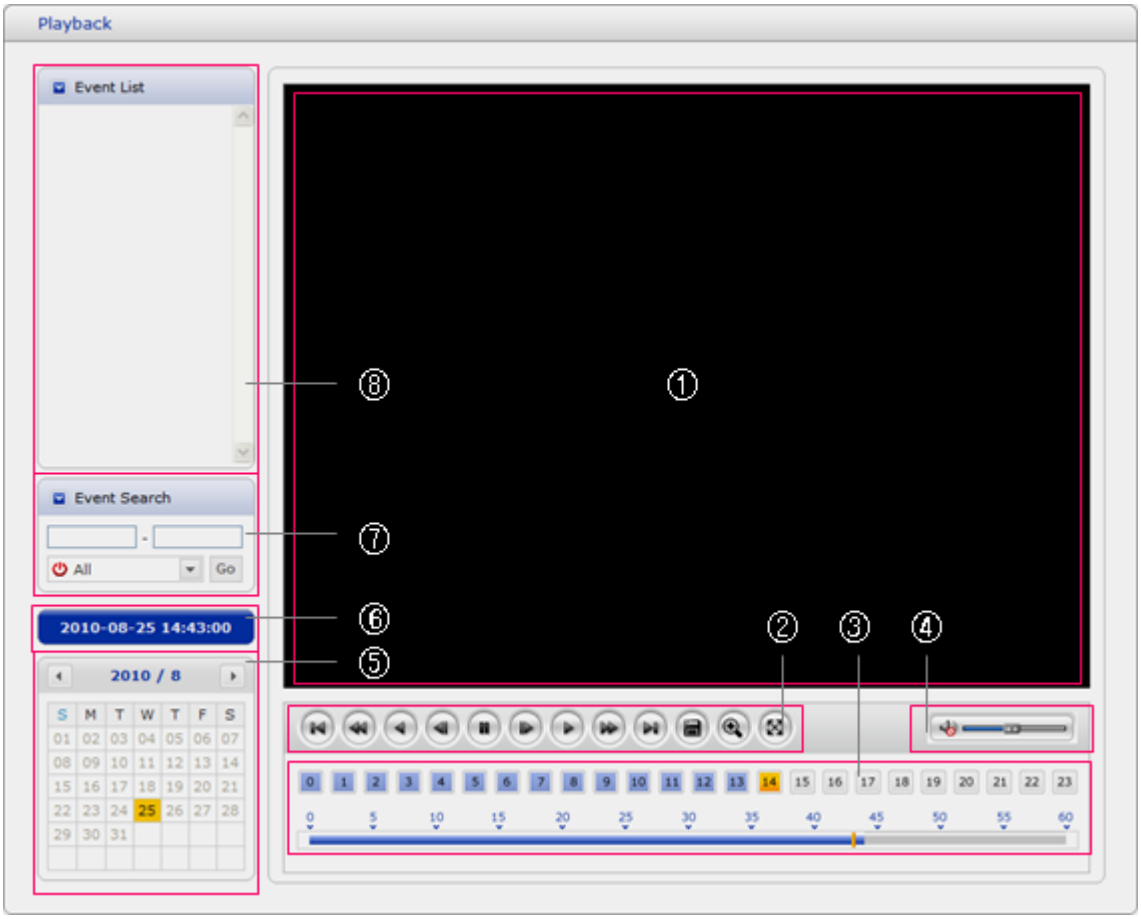


- **Logs**
  The Network Camera supports system log information. Click the **System Log** button to get the log data and the **Event Log** button for event information.

- **Reports**
  - **Server Report:** Click the Server Report button to get the important information about the server's status; this should always be included when requesting support.
  - **Parameter List:** Click the Parameter List button to see the unit's parameters and their current settings.

3.6 Playback

The Playback window contains a list of recordings made to the memory card. It shows each recording's start time, length, the event type used to start the recording; the calendar and time slice bar indicates if the recording existed or not.



The description of the playback window follows.

(1) Video Screen

The video screen is visible when playing the video clip in the Micro SD memory

(2) Playback Buttons

To view recording data in the SD local storage, select it from the list and click the Playback buttons.

- Go to the first: go to the beginning of the video clip.
- Fast backward play: fast play backward (rewind) of the video clip.
- Backward: play backward of the video clip.
- Step backward play: go back one frame of the video clip.
- Pause: pause playback of the video clip.
- Step forward play: go forward one frame of the video clip.
- Forward Play: play forward the video clip.
- Fast forward play: play fast forward of the video clip.

Clip copy: copy the video clip.

Zoom In: zoom in the video clip

Full Screen: display full screen of the video.

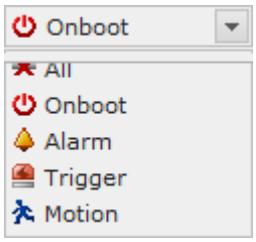
(3) Time Chart
Display an hour-based search screen for the chosen date. If there is recording data, a blue section will be displayed on a 24-hour basis.

(4) Speaker Control Bar
Use this scale to control the volume of the speakers.

(5) Search Calendar
Search results from the SD local storage in the network camera connected are displayed monthly. If there is a recorded data for a particular date, a blue square on the date will be displayed.

(6) Play Time
Displays time of the video playing.

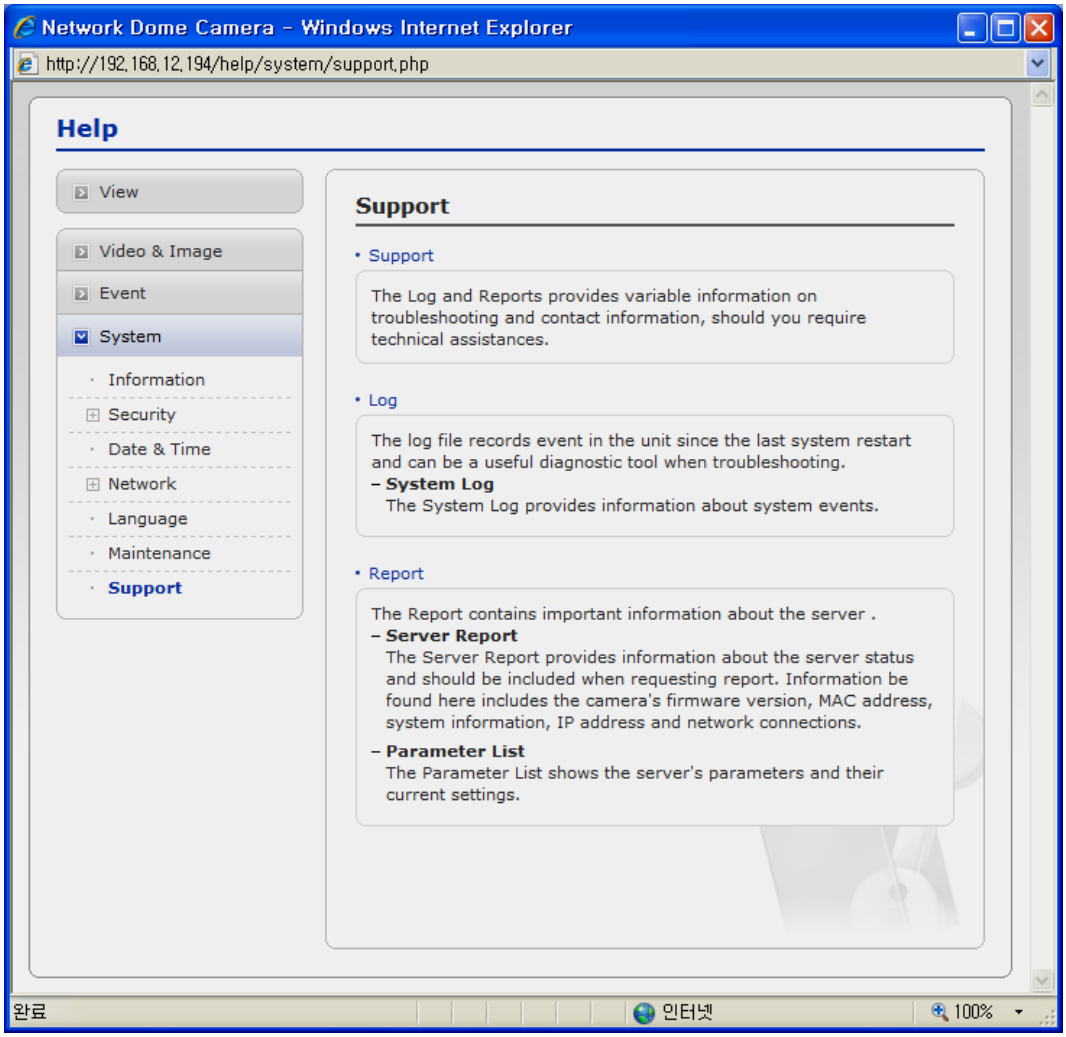
(7) Event Search Window
Select a search option in the drop-down list and click Go button. As an alternative, enter the time period for searching. If you click Start Date or End Date zone, the Search Calendar displays.



(8) Event List Window
Event List displays the event(s) that were recorded in the SD local storage. Select a list and click the Play button. The video clip will be played.

3.7 Help

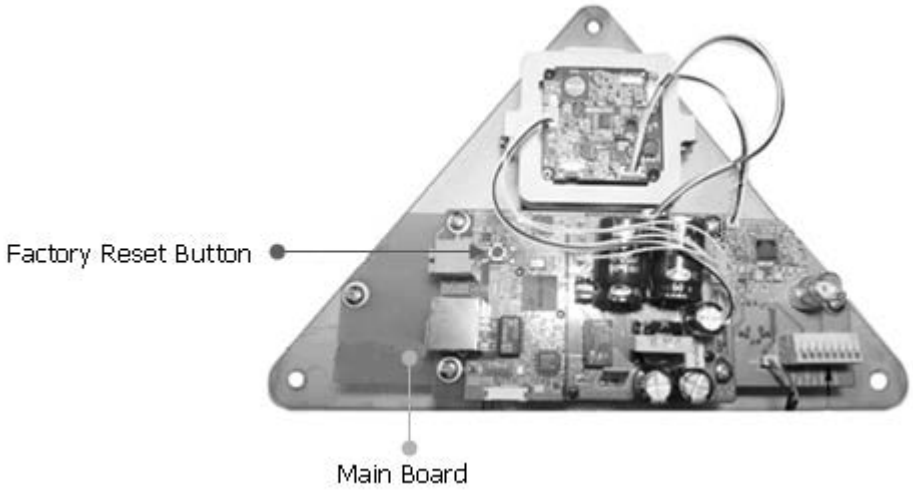
The Help information window is provided as a popup window so that users can open and read it without a need for log-in. It offers descriptions of settings and a Help page, so users can manipulate the Network Camera without having to reference manual.


Network Dome Camera - Windows Internet Explorer
http://192.168.12.194/help/system/support.php
Help
View
Video & Image
Event
System
Information
Security
Date & Time
Network
Language
Maintenance
Support
Support
• Support
The Log and Reports provides variable information on troubleshooting and contact information, should you require technical assistances.
• Log
The log file records event in the unit since the last system restart and can be a useful diagnostic tool when troubleshooting.
– System Log
The System Log provides information about system events.
• Report
The Report contains important information about the server .
– Server Report
The Server Report provides information about the server status and should be included when requesting report. Information be found here includes the camera's firmware version, MAC address, system information, IP address and network connections.
– Parameter List
The Parameter List shows the server's parameters and their current settings.
완료
인터넷
100%

3.8 Resetting to the factory default settings

To reset the Network Camera to the original factory settings, go to the Setup>System> Maintenance web page (described in “3.5.5 System > Maintenance”) or use the control button on the network camera, as described below:

- **Using the Reset Button**
  Follow the instructions below to reset the Network Camera to the factory default settings using the Reset Button.



1. Switch off the Network Camera by disconnecting the power adapter.
2. Open the rear cover.
3. Press and hold the Control Button (SW1) on the board with your finger while reconnecting the power.
4. Keep the Control button (SW1) pressed for about 2 seconds.
5. Release the Control Button (SW1).
6. The network camera resets to factory defaults and restarts after completing the factory reset. The unit now obtains the IP address automatically via DHCP.
7. Close the rear cover.

CAUTION: When performing a Factory Reset, you will lose any settings that have been saved.

4. Appendix

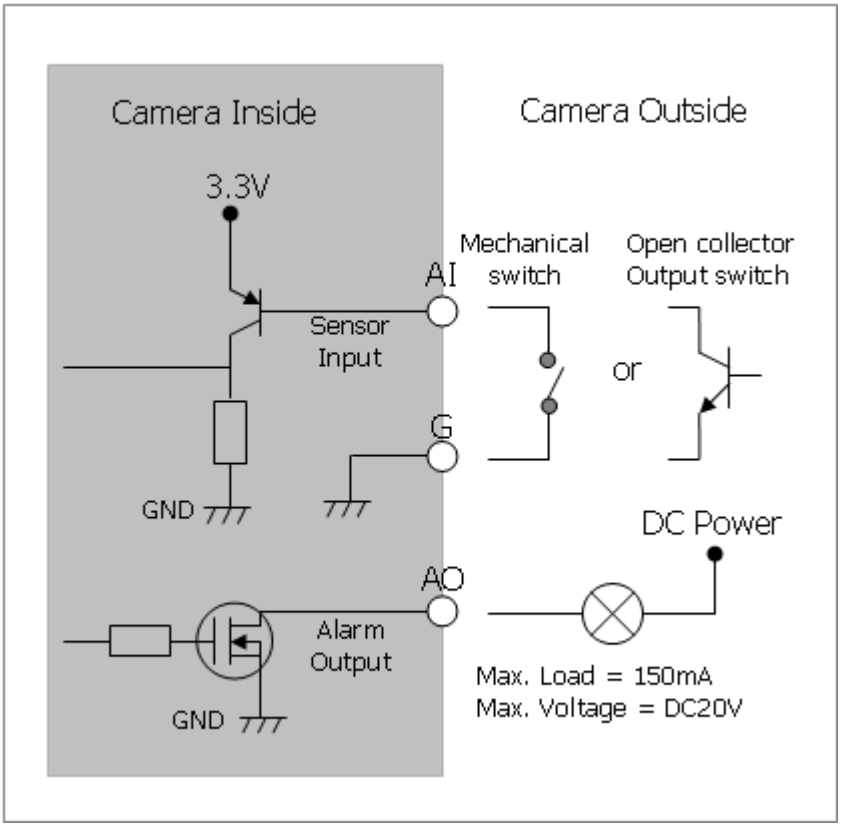
4.1 Troubleshooting

When troubleshooting if problems occur, verify the installation of the Network Camera with the instructions in this manual and with other operating equipment. Isolate the problem to the specific piece of equipment in the system and refer to the equipment manual for further information.

Problems/Symptoms	Possible Causes or Corrective Actions
The camera cannot be accessed by some clients.	If using a proxy server, try disabling the proxy setting in your browser. Check all cabling and connectors.
The camera works locally, but not externally.	Check if there are firewall settings that need to be adjusted. Check if there are router settings that need to be configured.
Poor or intermittent network connection.	If using a network switch, check that the port on that device uses the same setting for the network connection type (speed/duplex).
The camera cannot be accessed via a host name.	Check that the host name and DNS server settings are correct.
Not possible to log in.	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used. When attempting to log in, you may need to manually type in http or https in the browser's address bar.
No image using Refresh and/or slow updating of images.	If images are very complex, try limiting the number of clients accessing the camera.
Images only shown in black & white.	Check the Video & Image setting.
Blurred images.	Refocus the camera.
Poor image quality.	Increased lighting can often improve image quality. Check that there is sufficient lighting at the monitored location. Check all image and lighting settings.
Rolling dark bands or flickering in image.	Try adjusting the Exposure Control setting under AE and AWB part.
H.264 not displayed in the client.	Check that the correct network interface is selected in the Video & Image/Stream.
Multicast H.264 not displayed in the client.	Check with your network administrator that the multicast addresses used by the camera are valid for your network. Check that the Enable multicast checkbox are enabled in the System/Network/RTP tab. Checks with your network administrator to see if there is a firewall preventing viewing.
Multicast H.264 only accessible by local clients.	Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL value may need to be increased.
Color saturation is different in H.264 and Motion JPEG.	Modify the settings for your graphics adapter. Please see the adapter's documentation for more information.
Video cannot be recorded.	Check that the SD Card is inserted properly. Check that the SD Card is formatted properly.

4.2 Alarm Connection

The following connection diagram gives an example of how to connect a network camera.



4.3 Preventive Maintenance

Preventive maintenance allows detection and correction of minor faults before they become serious and cause equipment failure.

Every three-month, perform the following maintenance.

1. Inspect all connection cables for deterioration or other damage.
2. Clean components with a clean damp cloth.
3. Verify that all the mounting hardware is secure.

4.4 Product Specification

Main Item			Specification
Input Voltage			24 VAC, 12 VDC, Power over Ethernet IEEE 802.3af Class2/3
Power Consumption			9.0 Watts
CAMERA	Image sensor		1/3" Sony Super Had CCD II
	Total Pixels		811(H) x 508(V)
	Effective Pixels		768(H) x 494(V)
	Horizontal Resolution		600TVL
	S/N (Y signal)		More than 50dB (AGC OFF)
	Min. illumination		0.1 Lux(Color), 0.03 Lux(B/W), 0 Lux(BW at IR ON) @ F1.2 50IRE
	Shutter Speed		1/10,000 ~ 1/60(NTSC), 1/10,000 ~ 1/50(PAL),
	Fixed Lens	Focal Length	2.5mm
		Angle of View	H:104°, V:80°
NETWORK	Video Compression		Motion JPEG MPEG-4 Part2 H.264 (MPEG-4 Part 10) Profiles: H.264 MP and BP, MPEG-4 ASP and SP
	Video Resolutions		320x240 ~ 7040x480
	Frame Rate		30fps @ all resolutions
	Video Streaming		Simultaneously H.264(or MPEG-4) and MJPEG Controllable Frame Rate and Bandwidth VBR/CBR H.264 and MPEG-4
	Protocol		TCP/IP, UDP, IPv4/v6, HTTP, HTTPS, QoS, FTP, SNMP, uPnP, RTP, RTSP, RTCP, DHCP, ARP
	Security		Multi-user authority, HTTPS, IP Filtering, Privacy Zone
	Max. Connection		10
	API Programming Interface		API Supported, Open Platform Compatible: Milestone, ONVIF
	Alarm Triggers		Motion Detection, External Input, Manual Trigger
	Alarm Events		File upload via FTP and HTTP Notification via E-mail, HTTP and TCP External Output activation
	Video Buffering		Pre and Post Alarm
	Motion Detection		Yes, max. 8 programmable zone
	Network Time Synchronization		Yes
	SD Recording		Yes, Continuous/Schedule/Event
	Software Reset		Yes
	Factory Reset		Yes, Button/Web browser
	Auto Recovery		Yes
	Installation Tool		Yes, SmartManager
	Upgrade		Yes, Web browser/SmartManager
GENERAL	IR Illumination		36 IR LED illuminator(940nm not visibility) light up to 66ft(20m); intensity adjustable.
	Alarm Input		Terminal, 1 TTL input
	Alarm Output		Terminal, 1 open collector(max. 24V DC, max. 100mA)
	Audio In/Out		1 Mic / 1 Speaker(G.711)
	Ethernet		RJ-45 10BASE-T/100BASE-TX
	Operating Temperature		0°C ~ 50°C
	Operation Humidity		0~90% (non-condensing)
	External Dimension		380 mm x 320 mm
	Unit Weight		1600g
	Approval		FCC, CE

System Requirement for Web Browser

Operating System: Microsoft Windows 98, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows XP, or Microsoft Windows Vista

CPU: Over Pentium IV 2.4GHz, 512MB RAM, 10GB free disk or higher

VGA: AGP, Video RAM 32MB or higher (1024x768, 24bpp or higher)

Vicon Industries Inc.

For office locations, visit the website:

www.vicon-security.com

VICON